Addison-Wesley

الدار العربية للعلوم
Arab Scientific Publishers



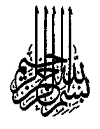
دليل سيمانتك إلى أمن الإنترنت في المنزل

الكتاب الوحيد حول أمن الإنترنت الذي ستحتاجه أبداً

من صانعي البرنامج
Norton AntiVirus

أندرو كونري موراي و فينسنت ويفر

أمن الإنترنت في المنــزل



يتضمن هذا الكتاب ترجمة الأصل الإنكليزي
The Symantec Guide to Home Internet Security
حقوق الترجمة العربية مرخّص بها قانونياً من المؤلف
Symantec Press
بمقتضى الاتفاق الخطي الموقّع بينه وبين الدار العربية للعلوم

أمن الإنترنت في المنزل

تأليف

أندرو كونري موراي - فينسنت ويفر



الدار العربية للعلوم

Arab Scientific Publishers

ISBN 9953-29-116-0

الطبعة الأولى

1427 هـ - 2006 م



الدار العربية للعلوم
Arab Scientific Publishers
عين التينة، شارع المفتي توفيق خالد، بناية الريم
هاتف: 860138 - 785108 - 785107 (1-961)
ص.ب: 13-5574 شوران - بيروت 2050-1102 - لبنان
فاكس: 786230 (1-961) - البريد الإلكتروني: asp@asp.com.lb
الموقع على شبكة الإنترنت: http://www.asp.com.lb

الترجمة: مركز التعريب والبرمجة، بيروت - هاتف 811373 (9611)
التنضيد وفرز الألوان: أبجد غرافيكس، بيروت - هاتف 785107 (9611)
الطباعة: مطابع الدار العربية للعلوم، بيروت - هاتف 786233 (9611)

المحتويات

مقدمة 13

الفصل الأول: فهم مخاطر الإنترنت 15
1-1 المحتالون والقراصنة 16
سرقة الهوية........ 17
السبام 17
الفيروسات والديدان........ 18
سبايوير، أدوير، وأحصنة طروادة 18
2-1 لماذا أنا؟ 19
كمبيوترك مورد لمهاجمة الكمبيوترات الأخرى 19
كمبيوترك كوسيلة اتصالات للمحتالين والمخادعين........ 20

الفصل الثاني: منع سرقة الهوية........ 23
1-2 كيف تتم سرقة هويتك........ 24
الهندسة الاجتماعية........ 25
الخداع 26
هجوم التصيد........ 26
مسجلات ضربات المفاتيح........ 27
سرقة البريد والبحث في سلة المهملات 28
2-2 منع سرقة الهوية 28
فكّر قبل أن تنقر 28
الأدوات المستخدمة لمنع سرقة الهوية 29
SSL........ 30
العلامات الأمنية........ 31
SpoofStick 33

2-3 استعادة الهوية المسروقة 33
2-4 لائحة التدقيق.. 34
ما يجب أن تفعله.. 34
ما يجب أن لا تفعله.. 35
2-5 موارد مساعدة.. 35
إجبار الشركات على التصريح عن اختراقات الخصوصية.. 36
تجربة شخصية مع سرقة الهوية 38
الفصل الثالث: جدران النار.. 41
3-1 الرزم، البروتوكولات، والمنافذ.. 42
IP وTCP.. 43
HTTP وHTML.. 44
3-2 ما الذي يمكن أن تفعله جدران النار 45
تنظيم الوصلات الواردة والصادرة 45
الإعدادات الأمنية 47
3-3 ما الذي لا يمكن لجدار النار أن يفعله.. 48
3-4 جدران النار المجانية.. 49
ويندوز XP سرفيس باك 2.. 49
ZoneAlarm من Zone labs 53
مراقبة البرامج المضادة للفيروسات.. 53
حماية البريد الإلكتروني 54
التنبيه والتسجيل.. 54
3-5 جدران النار التي يمكنك شراؤها.. 54
كيف يجب أن تختار؟.. 57
3-6 اختبار جدران النار.. 57
ShieldsUP! (www.grc.com) 57
اختبار الأمن من Symāntec (/www.symantec.com/homecomputing) 58
McAfee MySecurityStatus (/http://us.mcafee.com/MySecurityStatus).. 58
PivX Preview (www.pivx.com/preview).. 58
AuditMyPC (com.www.auditmypc).. 59

7-3 لائحة التدقيق.......... 59
ما يجب أن تفعله 59
ما يجب أن لا تفعله.......... 60
8-3 موارد مساعدة.......... 60

الفصل الرابع: التخلص من الضيوف غير المرغوبين، الجزء 1.......... 61
1-4 نمو المالوير 61
2-4 الفيروسات والديدان.......... 64
ما الذي يمكن أن تفعله الديدان والفيروسات؟.......... 67
3-4 البرمجيات المضادة للفيروسات 68
ما الذي يمكن أن تفعله البرمجيات AV 68
ما الذي لا يمكن أن تفعله البرمجيات AV.......... 69
4-4 طرق الحماية الأخرى.......... 70
استخدام جدار نار.......... 70
لا تفتح رسالة البريد الإلكتروني الغريبة.......... 71
لا تنقر على أي ارتباطات أو برامج في رسائل البريد الإلكتروني 72
حافظ على تحديث جميع البرمجيات.......... 72
5-4 ما الذي تفعله إذا ظهر لديك فيروس أو دودة.......... 72
كيف تعرف بأن كمبيوترك مصاباً.......... 73
كيف تزيل دودة أو فيروس 73
6-4 اختيار برمجيات مضادة للفيروسات.......... 74
7-4 لائحة التدقيق.......... 75
ما يجب أن تفعله.......... 75
ما يجب أن لا تفعله.......... 76
8-4 موارد مساعدة.......... 76
إزالة إصدار الدودة Beagle.......... 77

الفصل الخامس: التخلص من الضيوف غير المرغوبين، الجزء 2 81
1-5 ما هي سبايوير، أدوير وأحصنة طروادة؟ 81
تعريف سبايوير وأدوير 82
2-5 التحديات التقنية والقانونية لكشف وإزالة سبايوير وأدوير 87

هل تريد كعكة؟ 92
5-3 كيف تصيب برامج السبايوير، الأدوير وأحصنة طروادة كمبيوترك 94
من برنامج الاستعراض 95
من البرمجيات الأخرى 96
من البريد الإلكتروني 96
من الهندسة الاجتماعية 96
5-4 كيف تحمي نفسك من سبايوير، أدوير وأحصنة طروادة 96
استخدام البرمجيات المضادة للسبايوير والمضادة للفيروسات 97
احذر من الانتهازيين 99
البرمجيات المجانية المضادة للسبايوير 100
ما الذي يمكن أن تقوم به البرمجيات المضادة للسبايوير 101
ما الذي لا يمكن أن تقوم به البرمجيات المضادة للسبايوير 103
اشتبه بالبرمجيات المجانية 103
اقرأ الاتفاقية EULA 103
اضبط إعدادات برنامج الاستعراض 104
استخدام برنامج استعراض بديل 105
حافظ على البرمجيات محدثة 106
5-5 إزالة السبايوير، الأدوير وأحصنة طروادة 106
كيف تعرف أن كمبيوترك مصاب 106
استخدام HijackThis 108
5-6 لائحة التدقيق 109
ما يجب أن تفعله 109
ما يجب أن لا تفعله 110
5-7 موارد مساعدة 110
قراءة المادة الغامضة 111
الفصل السادس: فقط قل لا للسبام 113
6-1 تحقيق الأرباح من السبام 114
6-2 السبام، الخداع والتصيد 116
6-3 كيف يعمل مبرمجو السبام 117

شراء اللوائح 117
زواحف البريد الإلكتروني 118
هجوم القاموس/حصاد الدلائل 118
الخداع 118
الملقمات الوكيلة للسبام 118
الهندسة الاجتماعية 119
مرشدات الوب/علل الوب 119
6-4 طرق ترشيح السبام 120
مرشحات المحتوى/البحث عن الكلمة الأساسية 120
اللوائح السوداء 121
اللوائح البيضاء 121
التحليل المساعد 122
تواقيع السبام 122
التحدي والاستجابة 123
ترشيح بايسان 123
ترشيح السمعة 124
6-5 كيف تخفف من السبام 125
احذف الرسائل المشبوهة بدون فتحها 125
لا تجب على رسائل السبام أو التصيد 126
لا تنقر أي ارتباط في البريد غير الموثوق 126
اقرأ سياسات الخصوصية 126
لا تصرح عن عنوان بريدك الإلكتروني 126
غيّر عنوان بريدك الإلكتروني أو استخدم عدة عناوين بريد إلكتروني 127
لا تشترِ شيئاً من مرسلي السبام 127
أرسل تقريراً بالسبام والتصيد 128
6-6 الأدوات المضادة للسبام 128
6-7 لائحة التدقيق 131
ما يجب أن تفعله 131
ما يجب أن لا تفعله 131
6-8 موارد مساعدة 131

الفصل السابع: تأمين ويندوز 133
1-7 ويندوز XP سرفيس باك 2 134
مركز أمن ويندوز 135
إعداد جدار نار ويندوز 137
الحماية من الفيروسات 141
2-7 ثلاثاء الرقع 142
تأهيل التحديثات التلقائية 143
3-7 تأمين إنترنت إكسبلورر 144
أمن إنترنت إكسبلورر 145
التعامل مع أكتيف إكس 145
إعداد الخصوصية 149
حاجز الأطر المنبثقة 151
4-7 برامج الاستعراض البديلة 152
Firefox (org.www.mozilla) 153
Opera (www.opera.com) 154
5-7 التدقيقات الأمنية 155
ShieldsUp! (www.grc.com) 155
PivX Preview (com/preview.www.pivx) 155
Symantec Security Check (www.symantec.com/securitycheck) 156
6-7 إنترنت إكسبلورر 7.0 وويندوز فيستا 156
7-7 لائحة التدقيق 156
ما يجب أن تفعله 156
ما يجب أن لا تفعله 157
8-7 موارد مساعدة 157

الفصل الثامن: المحافظة على أمن عائلتك على الوب 159
1-8 ترشيح المحتوى غير المرغوب 160
المراقبة الشخصية 160
ترشيح محرك البحث 163
ترشيح إنترنت إكسبلورر 165

ترشيح برنامج الاستعراض البديل 170
تحكمات مزود الخدمة 170
التحكم بالسبام 171
8-2 المستغلون الجنسيون والإنترنت 171
منع الاتصالات غير المطلوبة 172
إرسال تقرير عن الدعوات الجنسية 173
برمجيات مراقبة الإنترنت 174
كيف يجب أن أختار؟ 174
8-3 الأغنية 3000$ ومشاكل مشاركة الملفات الأخرى 177
كيف يمكنهم العثور عليّ؟ 179
أمور أمن P2P 180
نظامي أم غير نظامي؟ 181
8-4 لائحة التدقيق 181
ما يجب أن تفعله 181
ما يجب أن لا تفعله 181
8-5 موارد مساعدة 182
علامات تدل على أن طفلك قد يكون في خطر على الوب 183

الفصل التاسع: أمن الاتصالات اللاسلكية وVoIP 185
9-1 عمل الشبكات اللاسلكية 186
9-2 الأمور الأمنية مع الشبكات WLAN المنـــزلية 188
تغيير SSID الافتراضي 191
إيقاف إذاعة SSID 192
تغيير كلمات المرور الافتراضية 192
تأهيل الترشيح MAC 192
البرمجيات الأمنية اللاسلكية 193
9-3 أمن الأماكن العامة 194
الشبكات اللاسلكية غير المحمية في الأماكن العامة 195
هجوم التوأم البغيض 197
لا تنفذ معاملات حساسة على شبكة لاسلكية في مكان عام 197

9-4 أمن الهاتف الخليوي وPDA 197
أنظمة التشغيل الجوالة وبلوتوث 198
مالوير الهواتف الخليوية 199
تأمين بلوتوث 200
أمن PDA 201
9-5 أمن VoIP 202
VoIP و911 203
9-6 لائحة التدقيق 204
ما يجب أن تفعله 204
ما يجب أن لا تفعله 204
9-7 موارد مساعدة 205

الفصل العاشر: الخصوصية والإنترنت 207
10-1 خيارات خصوصية الإنترنت 209
مبادئ التشفير 209
التواقيع الرقمية والشهادات الرقمية 210
تشفير البريد الإلكتروني 212
تشفير الملفات والمجلدات 215
مقنّعات الوب 215
10-2 التعامل مع سماسرة البيانات 216
Acxiom (www.acxiom.com) 217
ChoicePoint (www.choicepoint.com) 218
LexisNexis (www.lexisnexis.com) 219
10-3 لائحة التدقيق 219
ما يجب أن تفعله 219
ما يجب أن لا تفعله 220
10-4 موارد مساعدة 220

الخاتمة 223

مقدمة

شكراً لاختيارك هذا الكتاب. إذا كنت تبحث عن حل سريع وسهل للمحافظة على أمن كمبيوترات ويندوز من أخطار الإنترنت فقد حصلت على الكتاب المناسب. فهو مخصص للمستخدمين غير التقنيين، لذلك فهو يقدم تعليمات خطوة فخطوة بالإضافة إلى الأشكال المساعدة. وإذا كنت تعرف كيف تتجول على الوب وتحمّل البرمجيات، فإنك تملك جميع المهارات الضرورية لكي تستخدم الإنترنت بأمان.

في هذه الأيام يتم إجراء المزيد من المعاملات الحساسة عبر البريد الإلكتروني والإنترنت، بما في ذلك العمليات المصرفية على الوب، تجارة البضائع، الشراء من مواقع التجارة الإلكترونية وإدارة الحسابات الشخصية. وفي حين أن الإنترنت تبسط أداء هذا النشاط، ولكنها تطرح مخاطر أمنية أيضاً. فالمخاطر التقليدية مثل الفيروسات، الديدان وأحصنة طروادة ما تزال تهدد الإنترنت. وبالإضافة إلى ذلك فقد ظهرت مجموعة من التهديدات الكبيرة الجديدة، والتي يطلقها المجرمون الذين تدفعهم رغباتهم المادية، وأصبحت دورة حياتها أقصر وتستخدم وسائل جديدة لتسيير الهجوم. تطرح هذه التهديدات المروعة تحديات جديدة لأي شخص يستخدم الإنترنت.

وتحمل مواقع المعلومات والترفيه التي تبدو آمنة الأخطار أيضاً. على سبيل المثال، في دراسة أجرتها شركة أمن الإنترنت Symantec، أخذ الباحثون كمبيوتر ويندوز جديد، ووصلوه إلى الإنترنت بدون أي برمجيات حماية، واستعرضوا الوب. واستغرق الباحثون ساعة في استعراض فئات مختلفة من مواقع الوب، بما في ذلك مواقع التجارة الإلكترونية ومواقع الألعاب ومواقع جديدة. وللمفاجأة، فإن مواقع وب الأطفال كانت الأكثر في إرسال البرمجيات غير المرغوبة إلى الكمبيوتر – 359 أدوير في ساعة واحدة من التجول!

إن الهدف الرئيسي من هذا الكتاب هو مساعدتك على فهم أن استخدام الإنترنت يؤدي إلى التعرض إلى بعض المخاطر – على خصوصيتك وعلى بياناتك الشخصية وعلى استخدام

كمبيوترك وأدائه. سوف نبحث هذه المخاطر ونعرض بطريقة بسيطة ولكن شاملة كيف تخفف من تعرضك إلى هذه المخاطر.

وعلى العكس من كتب الكمبيوتر الأخرى التي تركز على مشكلتين كالسبام والفيروسات، فإن هذا الكتاب موجه لكي يكون مورداً شاملاً لأنواع كثيرة من المخاطر التي يواجهها مستخدمو الإنترنت. سوف تجد كمية كبيرة من المعلومات التي تهتم بإبعاد السبايوير، الديدان، الفيروسات، السبام والمتدخلين عن كمبيوترك؛ استخدام البريد الإلكتروني وبرامج الاستعراض بشكل آمن؛ المساعدة على حماية هويتك وخصوصيتك؛ حماية الوصلة اللاسلكية من المتجسسين والمحتالين؛ وإبعاد المواد الإباحية والاستغلال الجنسي عن أطفالك.

إذا قلّبت الفصول أو نظرت إلى جدول المحتويات، سوف ترى أن هذا الكتاب يضم كثيراً من التفاصيل - بما في ذلك الأشكال والتعليمات خطوة خطوة - عن طريقة اختيار واستخدام مختلف البرمجيات الأمنية، طريقة الاستفادة من المزايا الأمنية المبينة في ويندوز XP سيرفس باك 2، وطريقة حماية نفسك وعائلتك من المجرمين. كما أن العديد من البرمجيات الموصى بها في هذا الكتاب هي برمجيات مجانية.

إن هذا الكتاب مصمم لمساعدتك على حل مشاكل محددة. وبالتالي يمكنك أن لا تقرأه من البداية إلى النهاية. يمكنك أن تبدأ بأي فصل يتحدث عن الخطر الذي يهمك أكثر من غيره وتحصل على جميع المعلومات التي تحتاج إليها. وبالطبع فإن العديد من مخاطر الإنترنت قد أصبحت متداخلة، لذلك فإن هذا الكتاب يشير كثيراً إلى الفصول المتعلقة الأخرى.

يتم مقارنة الإنترنت غالباً بالطرق السريعة، لكنها أشبه بالمدينة - حيث نقضي معظم حياتنا. وهي أيضاً مدينة حجمها لا متناهي وأخطارها محدقة. لقد تم تصميم هذا الكتاب لكي يكون دليلاً موثوقاً إلى هذه المدينة فيمكنك أن تستمتع وعائلتك برحلة آمنة في الإنترنت.

الفصل الأول

فهم مخاطر الإنترنت

تصوّر هذا العالم بدون وجود الإنترنت. لم يمض على وجود هذه التقنية سوى سنوات قليلة وقد أصبحت أساسية في حياتنا ولا يمكننا التخلي عنها؛ نحن نعتمد عليها في الاتصالات، الترفيه، الوصول إلى المعلومات، والتجارة الإلكترونية. فالإنترنت وشبكة الوب العالمية تحقق لنا المتعة وسهولة الإنجاز.

لكن لسوء الحظ فقد أصبحت الإنترنت هدفاً للصوص والمخربين أيضاً. كما بدأت الإنترنت والوب بالتعرض للهجوم من عدد متزايد من المجرمين الذين يستخدمون قوة الشبكة العالمية من أجل تدمير ملفاتك، انتهاك أمورك الخاصة، الوصول إلى كمبيوترك أو تعطيله، وحتى سرقة أموالك وتعطيل بطاقات الاعتماد المصرفية.

ولكن على الرغم من وجود هذه المخاطر فإن تجنبها ليس مستحيلاً. وتتوفر الأدوات والتقنيات الضرورية لمنع هذه الأخطار، لذلك لا داعٍ للتخلي عن كل ما تقدمه الإنترنت. يرافقك هذا الكتاب كموجه، ومع ذلك فأنت لست بحاجة لأن تصبح خبيراً أمنياً؛ فإذا كنت قد استخدمت برنامج استعراض أو برمجيات تحتاج إلى التثبيت فإنك قد حصلت على المهارات الضرورية من أجل حماية نفسك وعائلتك.

يمكن تسهيل الأمر عليك بمقارنة كمبيوترك مع السيارة. عندما تقود السيارة فإنك تواجه أخطار محددة. فقد تتعطل سيارتك، قد تتسبب بوقوع حادث أو قد تتعرض للموت. ولكنك تقبل بتعريض نفسك إلى هذه الأخطار بسبب الفوائد الجمّة التي تحصل عليها من سيارتك وبسبب الإجراءات المتخذة للوقاية من هذه الأخطار: يوجد في سيارتك مكابح، أحزمة أمان وأكياس هوائية. وقد حصلت على شهادة قيادة وأنجزت إجراءات التأمين على سيارتك.

وعندما تستخدم الإنترنت فإنك تقبل بالتعرض إلى بعض الأخطار أيضاً: سرقة هويتك، الإصابة بالفيروسات، استلام البريد غير المرغوب والإصابة بالسبايوير، إلى آخره.

وحتى المواقع التي تبدو بأنها غير مؤذية كمواقع التجارة الإلكترونية المعروفة أو مواقع الترفيه على الوب فإنها قد تثبت برمجيات على كمبيوترك تولد نوافذ دعائية (وتقلل بذلك من أداء كمبيوترك) أو تتعقب استخدامك للإنترنت. على كل حال، يستخدم العديد من النـاس الإنترنت بدون اتخاذ أي إجراءات لتخفيف هذه المخاطر: لا يسـتخدمون جـدار نـار وبرمجيات مضادة للفيروسات، وليس لديهم أدنى فكرة عن المسيئين والقراصـنة الـذين يجوبون الإنترنت بحثاً عن ضحايا جدد. إن ذلك كالقيادة بدون وجود المكابح أو أحزمة الأمان. ويهدف هذا الكتاب إلى مساعدتك بفهم الأخطار التي تتعرض إليها من الإنترنت وتزويدك بالمعلومات الضرورية لمواجهتها.

يبحث هذا الفصل بأكثر مخاطر الإنترنت جدية ويشرح سـبب كـون الكمبيـوترات الشخصية المنـزلية أهدافاً مرغوبة لمجرمي الإنترنت. على كل حال، تذكر أنه بالإضـافة إلى التعرض إلى النشاط الإجرامي، فإن استخدام الإنترنت يؤدي إلى تعريض العائلـة إلى مخـاطر متنوعة مثل الوصول إلى مواقع التعري غير المرغوبة أو مواقع المقامرة على الوب أو الاستخدام غير الشرعي للموسيقا والأفلام التي تملك حقوق نسخ. وتشكل وصلات الإنترنت اللاسلكية في المنـزل أو في الأماكن العامة نقاط اختراق حساسة يمكن الوصول منـها إلى المعلومـات الخاصة باستخدام كمبيوتر محمول مزود ببطاقة اتصال لاسلكية. سـوف نتطـرق إلى هـذه المواضيع في الفصول القادمة.

1-1 المحتالون والقراصنة

تنقسم عمليات الهجوم ضد المستخدمين المنـزليين إلى فئـتين أساسـيتين: الاحتيـال والقرصنة. تهدف محاولات الاحتيال على الكمبيوتر إلى سرقة نقودك بتقديم منتجات مضـللة عن طريق رسائل البريد الإلكتروني أو الإعلانات المنبثقة أو بخـداعك لكشـف معلوماتـك الشخصية ومعلومات حسابك المصرفي مثل كلمات المرور. وتعتبر عمليـات سـرقة الهويـة وهجوم التصيد ورسائل السبام من الأمثلة الرئيسية على عمليات الاحتيال.

يحاول القراصنة التحكم بكمبيوترك لأهداف مشينة مثل تعقـب نشـاطك علـى الوب، تقديم الإعلانات غير المرغوبة، الإساءة إلى أداء كمبيوترك أو وصلة الإنترنـت أو استخدام كمبيوترك لإرسال السبام أو لبدء عمليات هجوم على أهداف أخـرى علـى الإنترنت.

يعتمد المجرمون بكثرة على البرمجيات الخبيثـة مـالوير في عمليـات القرصـنة علـى الكمبيوترات. تتضمن برامج المالوير الفيروسات، الديدان، أحصنة طروادة، السبايوير والأدوير. ويبحث هذا القسم في أكثر أنواع التهديدات شيوعاً على الإنترنت.

سرقة الهوية

إن سرقة الهوية هي إحدى تهديدات الإنترنت الأكثر ازدياداً في هذه الأيام – فقدان معلومات كأرقام حسابات البطاقات المصرفية وبطاقات الاعتماد، كلمات المرور، وأرقام الضمان الاجتماعي. لأنه يمكن استخدام هذه المعلومات في عمليات الاحتيال على الوب أو بدون اتصال.

تذكر لجنة التجارة الفيدارلية أنه تعرض أكثر من 10 مليون أميركي لسرقة الهوية في العام 2003. وفي الحالات القصوى، وصلت الخسائر المادية إلى عشرات الآلاف من الدولارات. وأدت إلى إيقاف العمل ببطاقات الاعتماد لبعض الضحايا، واستغرق الأمر شهوراً للعودة إلى حالة العمل السليمة.

إن هجوم التصيد هو أحد أشكال سرقة الهوية التي تعتمد على البريد الإلكتروني وعلى الوب. فتستقبل رسالة بريد إلكتروني تدّعي بأنها رسالة رسمية من مصرف شهير، شركة بطاقات اعتماد أو موقع تجارة إلكترونية. تخبرك الرسالة عن وجود مشكلة في حسابك وتطلب منك إرسال اسم المستخدم، رقم الحساب، وكلمة المرور من أجل التأكد من حالة الحساب. لكن هذه الرسالة كاذبة. وفي الحقيقة فإنك ترسل هذه المعلومات الحساسة إلى محتال وغالباً ما يكون في دولة بعيدة.

وتقدم نسخة محدثة من هذا الاحتيال ارتباط وب في رسالة البريد الإلكتروني. فإذا نقرت على هذا الارتباط يتم عرض صفحة تسجيل دخول مطابقة لصفحة تسجيل الدخول إلى المصرف، شركة بطاقات الاعتماد أو موقع وب التجارة الإلكترونية الذي تتعامل معه، مع الشعار المعتمد في الشركة. وبعد أن تكتب المعلومات المطلوبة ترى رسالة خطأ أو قد يطلب منك إدخال المعلومات مرتين. وفي هذه الأثناء يتم إرسال معلومات الدخول إلى ملقم يخضع لسيطرة المحتالين. فيستخدمون هذه المعلومات في عمليات الشراء أو سحب النقود باسمك. كما يمكنهم بيع معلوماتك الشخصية إلى مجرمين آخرين.

السبام

يشكل البريد غير المرغوب (المعروف بالسبام) وفقاً لبعض التقديرات حوالي 80 بالمائة من رسائل البريد الإلكتروني المتبادلة عبر الإنترنت. ومع أن السبام لا يسبب أذية كبيرة مثل مالوير أو سرقة الهوية، ولكنه بالتأكيد أحد المشاكل الأكثر إزعاجاً على الإنترنت. فيضيع وقتك من أجل حذف البريد غير المرغوب، بالإضافة إلى أن رسائل السبام تستخدم لغة أو صور غير لائقة. ويستخدم لصوص الهوية تقنيات السبام أيضاً لإرسال البريد الإلكتروني الخداعي.

الفيروسات والديدان

الفيروس هو شيفرة تنسخ نفسها ذاتياً وتعيش في المضيف، مثل مستند وورد. أما الدودة فهي برنامج ينسخ نفسه ذاتياً وينتقل من كمبيوتر إلى آخر. وغالبـــاً مـــا تحتـــوي الديـــدان والفيروسات على شيفرات خبيثة لقرصنة كمبيوترك، تدمير الملفـــات أو ســـرقة المعلومـــات الشخصية. تشير الأبحاث إلى أنه يتم إطلاق 500 فيروس ودودة جديدة في الإنترنـــت كـــل أسبوع. ويزداد عدد الفيروسات والديدان في الإنترنت كل عام بمعدل 400 بالمائة. كما تزداد مهارة مجرمي الإنترنت بإنشاء ديدان تنتشر بسرعة أكبر. على سبيل المثال، أصابت الـــدودة Blaster في عام 2004 100 000 كمبيوتر في خمس ساعات فقـــط. أمـــا الـــدودة SQL Slammer فقد انتشرت بسرعة كبيرة بحيث تضاعف عدد الكمبيوترات المصابة كل 8.5 ثانية خلال الدقيقة الأولى من حياتها.

سبايوير، أدوير، وأحصنة طروادة

إن سبايوير هو فئة متزايدة أخرى من مالوير. ويستخدم المصطلح سبايوير "spyware" غالباً لوصف مجموعة من البرامج التي تملك إمكانيات مختلفة، مثل تغيير رقم الهاتف الذي يتصل به مودمك عندما تعمل على الوب، حفظ ضرباتك على لوحة المفاتيح أو توجيـــه برنـــامج الاستعراض إلى مواقع غير مرغوبة.

أما أدوير فهو من فئة منفصلة من البرامج المرتبطة. يجمع أدوير المعلومات عنك وعـــن عاداتك في التحول على مواقع الوب من أجل خدمة الإعلانات الموجهة. يمكن أن تملأ برامج أدوير شاشة الكمبيوتر بالإعلانات المنبثقة، توجهك إلى مواقع بحث غريبة، وتســـيء إلى أداء كمبيوترك بشكل كبير.

وبخلاف الفيروسات والديدان، فإن سبايوير وأدوير لا تنسخ نفسها. وإنما تصاب بها عندما تزور موقع وب فيتم تحميلها إلى كمبيوترك بشكل سري. كما قد تأتي ســـبايوير وأدوير مع الأدوات المجانية مثل شاشات التوقف، برامج الطقس، وأشرطة أدوات برامج الاستعراض. وتشكل برامج مشاركة الملفات الصوتية والفيديوية مصدراً دائمـــاً لـــبرامج أدوير. وفقاً لاستطلاع Earthlink فإن الكمبيوتر المنـــزلي يحتوي بشكل وسطي على 25 برنامج سبايوير وأدوير.

توجد أيضاً أحصنة طروادة، وهي برمجيات حصلت على اسمها من حصـــان طـــروادة الأسطوري الذي أخفاه الجنود الإغريق لتهريب أنفسهم في مدينة "تروي" المحصـــنة بقـــوة. وعندما وصل الحصان إلى خلف جدران "تروي" بأمان، انتظر الجنود الإغريق هبـــوط الليـــل وانسلوا ليقتلوا جنود "تروي" في أسرّتهم ويسيطروا على المدينة.

في هذه الأيام لن تطعنك أحصنة طروادة وأنت نائم، لكنها تعطي مهاجم عن بعد التحكم الكامل بكمبيوترك. فيستطيع المهاجم أن يقرأ، يغير، ويحذف ملفاتك؛ يبدأ تشغيل برامج معينة؛ يثبت أو يزيل البرمجيات؛ ويجعل حياتك مع الكمبيوتر بائسة.

2-1 لماذا أنا؟

من الخطأ أن تظن أنك في مأمن من جرائم الإنترنت، حتى ولو لم يوجد على كمبيوترك سوى صور العطلات، بعض الملفات MP3 المحملة، بعض المستندات، ومفكرتك السرية. فمع أن محتويات القرص الصلب في الكمبيوتر لا تهمّ الأشخاص السيئين، لكن مجرمي الإنترنت لا يهاجمونك فقط بل يهاجمون آلاف أو مئات الآلاف من الكمبيوترات الأخرى في الوقت نفسه.

إن الهجوم على أعداد كبيرة من الكمبيوترات مهم لسببين. الأول، يمكن استخدام الكمبيوترات التي تم الوصول إليها كموارد لمهاجمة كمبيوترات أخرى. والسبب الثاني، مع ازدياد عدد ضحايا الاحتيال يزداد احتمال وقوع شخص جديد في الخديعة. دعنا ننظر إلى هاتين الفكرتين بشكل منفصل.

كمبيوترك مورد لمهاجمة الكمبيوترات الأخرى

إن كمبيوترك ووصلة الإنترنت هي أهداف قيّمة لأنه باجتماعها مع مئات أو آلاف الأجهزة الأخرى يمكنها أن تصبح سلاحاً يستخدمه المهاجم في تنفيذ هجومه ضد أهدافه التي غالباً ما تكون أهداف حكومية أو مؤسسات أعمال. فالأدوات البرمجية المؤتمتة تمسح أعداداً كبيرة من أجهزة الإنترنت، وتبحث عن نقاط الضعف في هذه الأجهزة. ثم تستخدم أدوات التدخل المؤتمتة نقاط الضعف بشكل متكرر لتثبيت البرامج الخبيثة التي تعطي المهاجم القدرة على التحكم من بعد بالأجهزة. تدعى غالباً الكمبيوترات التي تتم قرصنتها "زومبي" أو "يرقانة".

يستخدم مجرمو الإنترنت زومبي بطرق عديدة. أولاً، يستخدم المهاجمون أعداداً كبيرة من زومبي لبدء هجوم رفض الخدمة (DoS). يعمل هذا النوع من الهجوم بتوجيه حركة مرور كبيرة إلى الهدف، كموقع وب حكومي أو موقع شركة. ويمكن أن يؤدي الهجوم DoS الطويل بشكل كاف إلى قطع الاتصال عن الموقع المستهدف.

ويستخدم مجرمو الإنترنت الهجوم DoS كأحد أشكال الابتزاز على الإنترنت، فيتم تهديد مالكي مواقع الوب بتنفيذ هجوم على مواقعهم ثم يطلبون منهم الدفع وإلا سيتم إغلاق مواقعهم. إن هذه الخدع فعالة غالباً إذا كان الموقع المستهدف لا يفضل اللجوء إلى قوة القانون. فمواقع التعري، مواقع المقامرة، وبعض المواقع الأخرى هي أهداف مناسبة لهذا النوع من الهجوم.

وتسبب بعض البرمجيات الأخرى إلى أن يعمل كمبيوترك كجهاز توليد رسائل السبام. لقد أصبح توليد السبام عملية ضرب وهروب. فمرسلي السبام يبحثون بشكل دائم عن أجهزة جديدة يرسلون منها بريدهم التافه لأن مزودات خدمة الإنترنت (ISP) والمنظمات المضادة للسبام تتعرف على الكمبيوترات التي ترسل السبام وتحجزها بشكل سريع. ومن بين الطرق التي يستخدمها مرسلو السبام هي الولوج إلى الكمبيوترات المنـزلية واستخدامها لإرسال آلاف أو ملايين من الرسائل، ثم الانتقال إلى غيرها. والمشكلة بالنسبة إليك هي عدم تسليم بريدك الإلكتروني لأنه قد تم تأشير كمبيوترك كمصدر لرسائل السبام.

وبعض المجموعات، بما في ذلك مجموعات الجرائم المنظمة، تتعامل مع مزرعة كبيرة من الكمبيوترات التي تم الوصول إليها. وتؤجر هذه الأجهزة التي تم قرصنتها إلى من يدفع أكثر وذلك من أجل استخدامها لإطلاق هجوم رفض الخدمة أو لإرسال السبام. والكمبيوترات عالية السرعة والتي تستخدم وصلات إنترنت موصولة بشكل دائم هي كمبيوترات مفيدة على وجه الخصوص للمجرمين.

وأخيراً، يحقق الفيروس أو الدودة التي تنتشر بسرعة الشهرة لمنشئها. وكلما ازداد عدد الكمبيوترات التي تم الوصول إليها يكون هذا الأمر مدعاة للتفاخر.

كمبيوترك كوسيلة اتصالات للمحتالين والمخادعين

في العالم الحقيقي يحاول المجرم أن يصل إلى ضحية مهمة واحدة فقط في الوقت نفسه. ويوجد على الإنترنت عدد لانهائي من الضحايا المهمين. وتسهل الإنترنت على المجرمين إخفاء هويتهم بعد تطبيق خدعهم التي تبلغ العالم بأكمله.

كما تجعل خدمة البريد الإلكتروني هذه المهمة أسهل، لأنه حتى الكمبيوترات المحمية بشكل جيد تقبل الرسائل الإلكترونية. إن خدع البريد الإلكتروني، هجوم التصيد، والسبام تحقق عائداً منخفضاً (1 أو 2 بالمائة كاستجابة إجمالية)، ولكن إذا تم إرسال مئات الآلاف من الرسائل (أو ملايين الرسائل في حالة السبام)، فإن النتيجة تحقق ربحاً.

هناك خدعة بريد إلكتروني مشهورة يمثل فيها المحتالون دور أقارب وزير نفط أفريقي سابق. ويطلب هؤلاء الأقارب مساعدتك في نقل ملايين الدولارات إلى خارج البلاد، لقاء الحصول على نسبة مقبولة من هذه الملايين يتم دفعها مسبقاً من أجل المساعدة على تنفيذ المهمة. وكل ما يتوجب عليك فعله هو إعطائهم رقم حسابك المصرفي، وقد يطلبون إرسال بضعة آلاف من الدولارات لمساعدتهم بإنجاز المستندات.

لقد رأيت في رحلة إلى غرب أفريقيا جرت مؤخراً خمسة رجال في مقهى إنترنت

يرسلون مئات الرسائل كهذه، ويدعي جميعهم أن هذه الرسائل من زوجة مسؤول حكومي رفيع تم عزله. حاولت أن أحاور أحدهم لأنها ستكون قصة عظيمة، لكنه أغلق كمبيوتره وقال بأنه كان يراسل أصدقائه. كن حذراً فالشركات المنتجة للنفط في أفريقيا ليست الإغراء الوحيد: لقد تم استخدام العراق وجمهوريات الاتحاد السوفياتي السابق كطعم أيضاً، وكذلك البلدان التي عانت مؤخراً من كوارث طبيعية.

وهناك شكل مختلف من الاحتيال حيث يتظاهر المحتال بأنه امرأة في روسيا. ويبدأ بالتحادث مع رجال وضعوا أوصافهم في خدمة تواعد على الإنترنت. ويقدم صوراً (لإمرأة جذابة حتماً) ويدخل في مراسلات خاصة. ثم تعترف المرأة بحبها وتعبر عن رغبتها باللقاء. ولكنها محرجة من طلب النقود لمساعدتها بدفع نفقات الفيزا أو بطاقة الطائرة أو ماشابه. وفي النهاية تخسر الضحية الساذجة مئات، وحتى آلاف، الدولارات.

تبحث الفصول القادمة في الطرق الأفضل للحماية من تهديدات الإنترنت الدائمة.

الفصل الثاني

منع سرقة الهوية

إن قدرتك على تأكيد هويتك - أي تأكيد أنك هو الشخص الذي تدّعي هويته - هو أمر أساسي في الطريقة التي يتم بها أداء التجارة. فتستخدم دليلاً لكي تدل المؤسسة التي تتعامل بأنك هو الشخص الصحيح وبالتالي يتم ترخيص الخدمات أو الصفقات. إن الصور على بطاقات الهوية، سواء كانت شهادة قيادة أو بطاقة اعتماد، هي الطريقة الأكثر استخداماً للتحقق من الهوية في العالم الحقيقي.

أما على الإنترنت فإن هويتك تضم العديد من العناصر، مثل اسم المستخدم، كلمة المرور، أرقام التعريف الشخصية (PIN)، رقم الضمان الاجتماعي، أرقام حسابات مختلفة، والاسم الأول لأمك. تعمل الهوية الرقمية بافتراض أنك الشخص الوحيد الذي يعرف هذه المعلومات. لكن هذا الافتراض ساذج، ويسمح للخدع البدائية بالتوصل إلى أهدافها. فعندما تتابع أعمالك على الوب، لا يستطيع أي شخص أن يسألك عن بطاقة هوية عليها صورة.

في الأيام الأولى للإنترنت كانت أسوأ سرقة للهوية هي سرقة اسم المستخدم وكلمة المرور لمزود خدمة الإنترنت (ISP)، أي أن شخصاً آخر يمكنه التجول في الإنترنت على حسابك.

أما في هذه الأيام فنستخدم الإنترنت لتنفيذ مختلف المعاملات المالية، وبالتالي أصبحت سرقة الهوية أكثر خطراً. يمكن أن يستخدم المجرمون هويتك الرقمية من أجل فتح حسابات لبطاقات الاعتماد، تغيير عنوانك (لكي لا تبدأ باستلام فواتير مالية غريبة)، سحب قروض مصرفية، الحصول على عقود رهن، وإجراء المعاملات المالية، كل ذلك باستخدام اسمك. ويمكنهم أيضاً أن يبيعوا هويتك المسروقة إلى مجرمين آخرين في سوق الإنترنت السوداء. وتتراوح النتائج الخطيرة من تعطيل بطاقة الاعتماد إلى سرقة النقود من حسابك المصرفي.

إن خدع بطاقات الاعتماد هي النموذج الأكثر شيوعاً لسرقة الهوية. فيسرق المجرمون

المعلومات الشخصية لكي يستخدموها من أجل فتح الحسابات باسم شخص آخـــر، تزويـــر النفقات لشهر أو شهرين، وإلقاء البطاقة عندما تكشف شركة بطاقات الاعتماد الأمـــر. ورد في صحيفة نيويورك تايمز[1] أن إحدى حلقات سرقة الهوية سرقت ما يزيد عن 000 30 هويـــة وحصلت على عشرات الملايين من الدولارات خلال فترة عامين وذلك بإعادة بيع البضائع التي تم شراؤها ببطاقات اعتماد مسروقة. لقد كانت هذه الحلقة الإجرامية ناجحة جداً لأنها رشت موظفاً يمكنه الوصول إلى الهويات الرقمية للزبائن. فقام هذا الموظف السيئ باستغلال إمكانية الوصول المتاحة له في تجميع الهويات الرقمية، ثم باعها إلى العصابة التي فتحـــت الحســـابات الخادعة.

ويمكن تحقيق الأرباح حتى من عدد قليل من الهويات المسروقة. في عام 2004 تم اتهـــام شخص من فيرجينيا بسبب سرقة الأسماء والمعلومات الشخصية لعشرة أشخاص. لقد استخدم هذه المعلومات لفتح حسابات اعتماد واشترى بضائع بقيمة 000 85$ ثم باعها مجدداً علـــى eBay.

يهرب الأشخاص المسيئون مع القروض التي حصلوا عليها أو مع البضاعة التي اشتروها، بينما تهتم أنت بسداد الفواتير. وكونك لم تحصل على شيء مقابل هذه الفواتير لا يعفيك من الإيفاء بالتزامات سجلاتك المصرفية.

يبحث هذا الفصل بالطريقة التي يستخدمها المجرمون لسرقة هويتك، يذكر الخطوات التي يمكن اتخاذها لمنع سرقة الهوية، ويقدم نصائح حول طريقة استعادة هويتك إذا تم سرقتها وإساءة استخدامها.

2-1 كيف تتم سرقة هويتك

توجد طريقتان لسرقة هويتك الإلكترونية. في الطريقة الأولى يتم سرقة معلوماتك مـــن قاعدة بيانات المصرف، مزود الخدمة ISP، الموزعين، دور البيانات والهيئات الأخرى التي تحفظ المعلومات. ويتم سرقة هذه المعلومات في بعض الأحيان من مجرمين في عالم الكمبيوتر علـــى مستوى عالٍ من الخبرة. على سبيل المثال، في حزيران 2005 صدر تقرير عن مجرمي الكمبيوتر يصرح أنهم سرقوا معلومات الحسابات لأكثر من 000 200 بطاقة اعتماد من CardSystem Solutions، معالج دفع لبطاقات الاعتماد. وقد تم كشف معلومات أكثر من 40 مليون بطاقة أثناء الهجوم. كما يتم تسهيل عمل السرقة بالاشتراك مع موظف أو شريك يملك الوصول إلى البيانات، كما في القضية التي تم الإعلان عنها في ربيع 2005 حيث باع موظفون في أربعـــة مصارف، من بينها Bank of America and Wachovia، أكثر مـــن 000 670 ســـجل لحسابات الزبائن إلى أحد المجرمين.

ذهبت في 60 ثانية: سرقة الهوية هي وباء. هل يمكن إيقافه؟ الكاتـــب Timothy L.

O'Brien، نيويورك تايمز، 24 تشرين الأول 2004.

وأخيراً، يمكن الحصول على معلومات الهوية بتطبيق خدع قديمة جيدة. في إحدى الحالات التي حدثت مؤخراً، حاول المجرمون الوصول إلى بيانات الهوية بشكل شرعي من ChoicePoint، دار مقايضة بيانات. وبدلاً من تنفيذ عملية قرصنة معقدة، حصل المجرمون على شهادات أعمال من كاليفورنيا ثم اشتروا معلومات الزبائن عبر قنوات نظامية في ChoicePoint. (لمزيد من المعلومات حول آلية تنفيذ الهجوم على ChoicePoint، انظر إلى الشريط الجانبي قرب نهاية الفصل، "إجبار الشركات على التصريح عن اختراقات الخصوصية"). وكمستخدم كمبيوتر لا يمكنك فعل الكثير لحماية نفسك من هذا النوع من سرقة الهوية سوى مراقبة بيانات مصرفك وبطاقة اعتمادك والبحث عن أي معاملات غريبة، تدقيق سجلات بطاقة الاعتماد بشكل دوري، وانتقاء الشركات التي تقيم أعمالك معها. وفي بعض الحالات يمكنك أن تدقق فيما إذا كانت معلوماتك محفوظة في شركات دور مقايضة البيانات. انظر إلى الفصل العاشر، "الخصوصية والإنترنت" لمزيد من المعلومات.

الطريقة الثانية لسرقة الهوية هي أن يسرقها المهاجم منك مباشرة أو أن يخدعك لكي تعطيه هذه المعلومات. وفي العديد من الحالات تكون هذه الطريقة أسهل بكثير من محاولة اختراق شبكة محصنة (مع أن قرصنة قواعد بيانات شركة قد يكون سهلاً جداً لشخص خبير ودؤوب، لكن هذا الموضوع لكتاب آخر).

في معظم الحالات يمكنك أن تواجه هذه الطريقة الثانية لسرقة الهوية. ولكن قبل أن نتحدث عن ذلك، سنذكر بعض المعلومات عن الطرق المختلفة لسرقة الهوية.

الهندسة الاجتماعية

إن الهندسة الاجتماعية هي طريقة تقنية لوصف خداع الناس. تعتمد الهندسة الاجتماعية على الثقة الفطرية بالأشخاص الآخرين (حسناً، السذاجة)، خصوصاً في حالات معينة إذا كانوا يرتدون لباساً موحداً ويضعون لوحة اسمية أو يرتدون بذة عمل.

يستخدم الخبراء الأمنيون والمجرمون (ندعوهم أحياناً خبراء الاختراق) الهندسة الاجتماعية لاختراق موقع محمي. على سبيل المثال، يرتدي خبراء الاختراق بذة وربطة عنق في مكتب معين ويتجولون، ونادراً ما يوقفهم أي شخص. على سبيل المثال، هل سألت مرة عن اللوحة الاسمية لموظف غريب إذا كان يتبعك ويدخل من باب يحتاج إلى استخدام بطاقة دخول؟ وإذا سألته فعلاً وقال لك أنه قد نسي لوحته الاسمية على مكتبه، ما الذي ستفعله عندئذ؟ سوف تبتسم على الأغلب وتدعه يمر.

ربما يكون المهندس الاجتماعي سيء السمعة الأكثر شهرة هو كيفين ميتينيك، مجرم مدان نفذ عملياته الكبيرة بالاعتماد على الهاتف وليس على مهاراته أو الخدع البرمجية. لقد

كانت أحد أهدافه المفضلة هي شركة الهاتف. يتصل بشركة الهاتف ويتظاهر بأنــه مهنــدس فيحثّ الشخص الذي يجيبه على الإدلاء بجميع المعلومات المفيدة، مثل كلمات المرور التي تمكنه من الوصول إلى أنظمة الكمبيوتر الحساسة. يمكنك أن تقرأ المزيد عن عمليات ميتينيك وكيف تم القبض عليه في الكتاب، ملاحقة كيفين ميتينيك والقبض عليه، أكثر المطلوبين في أميركــا بسبب جرائم الكمبيوتر – بلسان الشخص نفسه، الكاتب تســوتومو شــيموميرا وجــون ماركوف.

تعتمد الكثير من خدع سرقة الهوية على درجة معينة من الهندسة الاجتماعية. وأكثــر الطرق استخداماً هي رسائل البريد الإلكتروني الخادعة التي توهم بأنها صادرة عــن مؤسســة شرعية أو أنها خدمة مجانية على الإنترنت كبرمجيات مشاركة الملفات، الألعاب أو الأدوات التي تحتوي أيضاً على برامج خبيثة يمكن استخدامها لسرقة المعلومات السرية.

الخداع

يعني الخداع على الإنترنت إنشاء نسخة زائفة من شيء ما مثل موقع وب أو عنوان بريد إلكتروني. على سبيل المثال، ينشئ العديد من مجرمي سرقة الهوية مواقع وب خادعة تبدو مطابقة للموقع الحقيقي ويخدعون المستخدمين بالدخول إلى هذه المواقــع. وبعــد الدخول إلى أحد هذه المواقع، يسجل المستخدمون الدخول مع اسم المســتخدم وكلمــة المرور، فيجمعها المجرمون ويستخدمونها في الوصول إلى موقع الوب الحقيقي. يدعى ذلك بخداع موقع الوب. يستخدم مرسلو السبام أيضاً خداع عناوين الإجابــة علــى البريــد الإلكتروني – أي أنهم يضعون في رسائل السبام التي يرسلونها عنوان بريد إلكتروني للإجابة وهو غير موجود فعلياً.

هجوم التصيد

هذا النوع من الهجوم على الإنترنت شائع جداً وهو مخرب جداً. تبــدأ العديــد مــن عمليات هجوم التصيد برسالة بريد إلكتروني. على سبيل المثال، يرسل مجــرم آلاف رســائل السبام توهم بأنها صادرة عن مصرف، شركة بطاقات اعتماد، مزود خدمة ISP أو شــركة تجارية إلكترونية (مثل eBay وPayPal). بعض رسائل البريد الإلكتروني لهجوم التصيد تكون خدعة واضحة، لكن بعض الرسائل الأخرى هي أعمال في منتهى الدقة، تحمل شعار الشركة ومكتوبة بلغة الشركات التسويقية.

تبدو رسائل التصيد متشابهة بشكل عام. فتخبرك عن وجود مشكلة مع حســابك يجب أن تعالجها على الفور، وتتضمن ارتباطاً إلى ما يشبه صفحة تسجيل الــدخول إلى موقع وب. وفي الحقيقة يكون الموقع مزيفاً وهو عبارة عن نسخة مطابقة للموقع الحقيقي،

يتم استضافته على ملقمات لدى المجرمين. وفي حالات أخرى، يكون الارتباط صحيحاً، لكن المجرمين يتلاعبون بنظام عنونة الإنترنت لتوجيهك إلى موقعهم الخادع (يدعى ذلك أحياناً "فارمينغ").

إذا نقرت الارتباط، تجد صفحة تسجيل دخول مطابقة للموقع النظامي مع حقول إدخال اسم المستخدم، رقم الحساب وكلمة المرور. ومعظم المواقع الخادعة تكون طماعة وتسألك عن معلومات أخرى مثل رقم الضمان الاجتماعي. إذا أردت أن تعالج أي مشكلة في حسابك يجب عليك – الضحية – أن تدخل المعلومات بكل طواعية. وحسب درجة ذكاء سارق الهوية فقد ينقلك عملياً إلى الموقع الحقيقي. أما السارق الأقل ذكاءً فيعرض عليك رسالة خطأ. وخلال ذلك يتم نقل معلوماتك إلى ملقم يسيطر عليها المجرمون.

هناك نوع من الهجوم مقلق جداً يفسد فيه المجرم صفحة تسجيل الدخول لموقع وب نظامي. أي أنه عندما تكتب www.yourbank.com في برنامج الاستعراض يتم توجيهك إلى الموقع النظامي، وعندما تدخل معلوماتك، تقوم شيفرة خبيثة – أدخلها المجرم سابقاً في موقع الوب – بالتقاط المعلومات وإرسالها إلى كمبيوتره. إنها عملية مخيفة، لأنه ولو نفذت كل شيء بشكل صحيح فإن الخلل في طريقة إنشاء المواقع النظامية يجعلها عرضة لهذا الهجوم وليس بوسعك أي شيء حيال ذلك.

مسجلات ضربات المفاتيح

إنها برامج تتعقب كل ضربة على لوحة المفاتيح. ويتم إرسال هذه المعلومات إلى مهاجم بعيد، يمسح المعلومات من أجل بتات البيانات المفيدة ككلمات المرور وأرقام الحسابات. تأتي بعض مسجلات ضربات المفاتيح مع لائحة بمواقع الوب، مثل مواقع المصارف والتجارة الإلكترونية، وتبدأ بتسجيل ضربات المفاتيح فقط عندما تكتب هذه المحددات URL في برنامج الاستعراض. يتم بحث مسجلات ضربات المفاتيح بتفصيل أكبر في الفصل الخامس "التخلص من الضيوف غير المرغوبين، الجزء 2: سبايوير، أدوير وأحصنة طروادة". ويتم استخدامها بشكل رئيسي من أجل سرقة الهوية.

تزداد خبرة مهاجمي التصيد كثيراً، فيستخدم العديد منهم برمجيات خبيثة في رسالة البريد الإلكتروني المرسلة. تقوم هذه البرامج بأشياء مختلفة، بعضها مسجلات ضربات المفاتيح (سوف يتم نقاشها في الفقرة اللاحقة) وبعضها الآخر يرشد كمبيوترك إلى موقع خادع حتى لو كتبت عنوان موقع نظامي في برنامج الاستعراض. تم اكتشاف أحد البرامج يحتوي على لائحة بمواقع المصارف. وإذا ذهبت إلى أحد هذه المواقع الموجودة على اللائحة، فإن البرنامج يفتح برنامج استعراض غير مرئي خلف البرنامج الذي تراه على الشاشة، وذلك بعد تسجيل الدخول. ثم يدقق البرنامج ميزانيتك وينقل النقود إلى حساب يسيطر عليه المجرم.

سرقة البريد والبحث في سلة المهملات

يمكن أن يسرق المجرمون البريد الوارد والصادر من صندوق بريدك. فكر بجميع المعلومات المفيدة الموجودة في مغلف الدفع لبطاقة الاعتماد: الاسم، العنوان، رقم الهاتف، رقم بطاقة الاعتماد ورقم الحساب. إذا أمكنك، احصل على صندوق يمكن قفله للبريد الوارد وألق رسائلك الصادرة في صندوق البريد الموجود في المدينة.

توجد طريقة أخرى غير مستحسنة ولكنها فعالة وهي البحث في سلة المهملات. فالناس يلقون عادةً كل المعلومات المفيدة والمهمة، مثل بيانات الحساب المصرفي. ويمكن للمهاجمين الحصول على هذه المعلومات بالبحث عنها في مهملاتك. والطريقة الأفضل لمنع حدوث هذا النوع من السرقة هو بتمزيق المستندات المهمة قبل رميها.

وبمناسبة الحديث عن رمي الأشياء، يجب أن تأخذ وقتك لكي تمسح القرص الصلب لأي كمبيوتر تستغني عنه. إن حذف الملفات أو تهيئة القرص الصلب ليس كافياً؛ لأنه توجد العديد من البرمجيات التي يمكن استعادة المعلومات المحذوفة. تحتاج إلى برمجيات خاصة تخلط البيانات الموجودة على القرص. ومن هذه الأدوات Web Eraser، WipeDrive، و O&O SafeErase. وهناك شركة تدعى WindsorTech تمسح القرص الصلب عبر الإنترنت. انظر إلى www.eraseyourharddrive.com.

2-2 منع سرقة الهوية

توجد طرق عديدة لمنع سرقة الهوية على الوب. يستخدم بعضها التقنية، ولكن معظمها يعتمد على المفهوم العام. سوف نبدأ من المنع الذي يعتمد على المفهوم العام لأنه فعال ومجاني. ثم ننتقل إلى الخيارات التقنية.

فكّر قبل أن تنقر

كما ورد ذكره، تعتمد العديد من عمليات سرقة الهوية على الهندسة الاجتماعية والبريد الإلكتروني الخادع. ودفاعك الأفضل ضد هذه الأنواع من الهجوم هو اعتماد مبدأ الشك بالنسبة لأي رسالة تدّعي أنها صادرة من موقع تجارة إلكترونية أو من مؤسسة مالية. يمكن أن تساعد النقاط التالية على صد هجوم التصيد المعتمد على البريد الإلكتروني:

- إن المؤسسات النظامية لا ترسل بريد إلكتروني يسألك عن معلومات الحساب.
- تولي الشركات عناية كبيرة لتجنب الأخطاء الإملائية والنحوية في رسائلها مع الزبائن. انتبه إلى الرسائل التي تحتوي على أخطاء إملائية أو نحوية وجمل غريبة.

- لا تنقر أي ارتباط موجود في الرسالة. انظر بعناية إلى هذه الارتباطات. فقد تحتوي على أسماء غريبة.
- إذا كنت تظن أنه قد يوجد فعلاً مشكلة في حسابك، فإن الخيار الأفضل هو إجراء حديث هاتفي مع خدمة الزبائن. وإذا لم يكن ذلك ممكناً أغلق رسالة البريد الإلكتروني واكتب المحدد URL في برنامج استعراض الوب بنفسك. لا تقص وتلصق المحدد من رسالة البريد الإلكتروني.
- استخدم البرمجيات أو أداة أخرى، كما يتم شرحه لاحقاً في هذا الفصل، لكي تعرف فيما إذا كان هذا الموقع خادعاً.
- إذا حصلت على بريد إلكتروني يدّعي بأنه من موقع تجارة إلكترونية أو مصرف ليس لك أعمال معه، احذف رسالة البريد الإلكتروني دون فتحها. تحتوي العديد من رسائل التصيد على فيروسات أو مالوير تصيب كمبيوترك إذا فتحت الرسالة.
- استخدم برمجيات مضادة للفيروسات، وحدّثها باستمرار وتأكد من إعدادها لمسح البريد الإلكتروني بشكل تلقائي.
- دقق بيانات مصرفك وبطاقة الاعتماد بشكل دوري. ويمكنك أيضاً تدقيق تقرير بطاقة الاعتماد لمراقبة أي عمليات غير عادية. يمكنك شراء تقرير بطاقة الاعتماد من ثلاث وكالات تقريرية رئيسية لبطاقات الاعتماد – Experian، Equifax وTransUnion – كما أن هذه الوكالات مطالبة بالقانون أن تزودك بتقرير بطاقة اعتماد مجاني مرة في السنة. لكي تحصل على نسخة مجانية، اذهب إلى www.annualcreditreport.com أو اذهب إلى مواقع الوكالات التقريرية. يمكنك الحصول على تقريريك على الوب أو عبر البريد الحكومي. ويمكنك طلب نسخة مجانية عن التقرير عبر الهاتف بطلب الرقم 877-322-8228.

الأدوات المستخدمة لمنع سرقة الهوية

توجد العديد من الأدوات، إلى جانب الحدس العام، تساعد في منع سرقة الهوية. وتوجد في أعلى اللائحة البرامج المضادة للفيروسات والمضادة للسبايوير. ويجب أن تبقي البرمجيات المضادة للفيروسات AV محدثة بشكل مستمر، بسبب وجود فيروسات أو شيفرات خبيثة في العديد من رسائل التصيد. يجب أن تستخدم أيضاً البرمجيات المضادة للسبايوير (أو تتأكد من أن البرمجيات المضادة للفيروسات تكشف السبايوير) وتمسح كمبيوترك بشكل دوري. تكشف البرمجيات المضادة للسبايوير البرامج مثل مسجلات ضربات المفاتيح، التي تتعرف على عملية المجرم لأخذ البيانات الشخصية. يتم تغطية سبايوير والحلول المضادة للسبايوير بمزيد من التفصيل في الفصل الخامس.

يجب أن تتخذ خطوات لتحصين برنامج الاستعراض الذي تستخدمه مـــن عمليـــات التحميل خلال التجوال، والتي يتم فيها تثبيت مالوير على كمبيوترك وذلك من مواقع الــوب الخبيثة أو التي تم السيطرة عليها. يتم تغطية أمن برنامج الاستعراض في الفصل السابع، "تأمين ويندوز".

توجد أدوات أخرى تتعامل بالتحديد مع عمليات التصيد وسرقة الهوية. تناقش الأقسام التالية بعض ما تريد معرفته. بعضها مجانية والأخرى يجب أن تدفع من أجلها.

SSL

طبقة المقابيس المحمية (SSL) هي بروتوكول يؤهل الإرسال المرمز للمعلومـــات عـــبر HTTP (تعني HTTP بروتوكول نقل النصوص الفائقة، آلية الاتصالات المستخدمة في الوب). وتؤهل SSL أيضاً استخدام الشهادات الرقمية فيستطيع برنامج الاستعراض التأكد من صحة موقع الوب. إن الشهادة الرقمية هي نموذج من التحقق من الصحة الإلكتروني ينص أن فريق ثالث قد تحقق من حامل الشهادة التي يدّعي بها. فعندما تتحول إلى موقع مصرفك وتســجل الدخول لكي تنجز معاملة مصرفية، ينظر برنامج الاستعراض إلى الشهادة الرقمية للموقع لكي يضمن أن www.onlinebank.com هو بالفعل www.onlinebank.com.

تملك جميع برامج الاستعراض القدرة على استخدام SSL – ولا تحتاج إلى تنفيــذ أي شيء لتأهيلها.

هناك طريقتان لكي تعرف إذا كانت SSL مستخدمة أم لا. يظهر العنوان في شـــريط برنامج الاستعراض //:https بدلاً من //:http. (HTTP هو النسخة المحمية من بروتوكول نقل النصوص الفائقة). وترى أيضاً رمز قفل في الزوايا الدنيا اليمنى من برنامج استعراض الوب.

على كل حال، وجود رمز القفل أو https في شريط برنامج الاستعراض لا يضمن أن الموقع ليس خادعاً. فبإمكان المجرمين تسجيل موقع واستخدام SSL كما في الأعمال النظامية. يجب أن لا تنجز معاملات على الوب إلا مع مواقع وب تستخدم SSL، لكن ليس كل موقع يستخدم SSL هو موقع نظامي.

بالإضافة إلى ذلك، فإن استخدام مؤسسة نظامية للبروتوكول SSL لحماية نقل بياناتك لا يضمن أنها تحفظ معلوماتك بشكل آمن. فالمجرمين يهاجمون قواعد بيانات الشركات بشكل دوري لسرقة المعلومات. ولكن لا يعني ذلك أن تقلع عن استخدام التجارة الإلكترونيـــة، لأن أرقام حسابات بطاقات الاعتماد التي تستخدمها في المخازن الحقيقية توجد أيضاً في قواعـــد بيانات يمكن سرقتها. المشكلة ليست في النقل الآمن بل هي في صعوبة الحفظ الآمن وتـــأمين الحراسة الإجرائية.

العلامات الأمنية

كما ورد ذكره سابقاً، أحد المشاكل مع التجارة الإلكترونية هي أن نظام التحقق من الصحة يعتمد على معلومات مثل اسم المستخدم وكلمة المرور التي يمكن تخمينها أو الحصول عليها بالخديعة. يمكن مواجهة هذه المشكلة باستخدام التحقق من الصحة الثنائي، الذي يجمع بين شيء تعرفه (اسم المستخدم أو كلمة المرور) مع شيء تملكه. أحد الأمثلة على التحقق من الصحة الثنائي هو بطاقة ATM. العامل الأول هو الرقم PIN (شيء تعرفه). والعامل الثاني هو بطاقة المصرف نفسها (شيء تملكه). فالرقم PIN عديم الفائدة للمجرم بدون البطاقة، كما أن البطاقة عديمة الفائدة بدون الرقم PIN.

إن التحقق من الصحة الثنائي مفيد على وجه الخصوص لمنع سرقة الهوية على الوب لأنه حتى لو استطاع المجرم سرقة اسم المستخدم وكلمة المرور، لا يمكنه استخدام حسابك بدون حيازة العامل الآخر.

في المؤسسات التي تحتاج إلى درجة كبيرة من الأمن أو المؤسسات الحكومية يتم تنفيذ التحقق من الصحة الثنائي باستخدام أحد ثلاثة بنود:البطاقة الذكية، القياس البيولوجي أو العلامة. البطاقة الذكية هي قطعة من البلاستيك بحجم بطاقة الاعتماد. وتحتوي على رقاقة تحفظ شهادة رقمية تحدد بشكل فريد حامل البطاقة ويتم الوصول إليها باستخدام رقم PIN. أما القياس البيولوجي فهو إصدار رقمي من المميزات الفيزيائية مثل بصمة الإصبع أو صورة لشبكية العين أو الحدقة. والعلامة هي جهاز صغير يولد رقم عشوائي بفترات نظامية؛ ويكتب المستخدمون الرقم مع اسم تسجيل الدخول وكلمة المرور.

إن آلية التحقق من الصحة الثنائي الأكثر انتشاراً في عالم التجارة الإلكترونية هي العلامات. وذلك لأن البطاقة الذكية والقياسات البيولوجية تحتاج إلى قارئات خاصة يجب تثبيتها على كمبيوتر المستخدم. مع مرور الزمن سوف يباع كثيراً من الكمبيوترات التي تحتوي على هذه الأجهزة، أما الآن فإن استخدام العلامات أسهل لأنها لا تحتاج إلى تثبيت عتاد إضافي في الكمبيوتر.

SecurID هي العلامة المعروفة بشكل واسع، أنشأتها شركة تعنى بقضايا الأمن تدعى RSA. تبدو العلامة SecurID كحاسبة جيب صغيرة مع شاشة صغيرة وبدون أزرار. تولد العلامة رقم جديد بست خانات بفترة دورية محددة بشكل مسبق (مثلاً كل 60 ثانية). تولد الرمز بست خانات باستخدام خوارزمية رياضية تجمع رقم فريد يدعى قيمة البذرة مع زمن الساعة. تملك كل علامة مستقلة قيمة بذرة، لذلك لا تولد أي علامتان الرقم نفسه.

عندما يريد مستخدم أن يسجل الدخول إلى موقع يستخدم التحقق من الصحة الثنائي،

يتم توجيهه لإدخال رقم بست خانات مع اسم المستخدم وكلمة المرور. ويوجد في المؤسسة ملقم تم برمجته ليعرف قيمة البذرة وزمن الساعة لكل علامة، فيمكنه أن يقرر أن الرمز سداسي الخانات مقبول.

يعرف الملقم أيضاً أي مستخدم مقترن مع أي علامة، فيمكنه أن يطـابق المعـرف ID للمستخدم مع الرمز سداسي الخانات الذي تم توليده بالعلامة. وأخيراً يقبل الملقـم الأرقـام سداسية الخانات التي تم توليدها ضمن إطار زمني محدد فقط (على سبيل المثال، ضمن الدقائق الخمسة الأخيرة).

فإذاً كيف تساعد العلامات على سرقة الهوية؟ لنفترض أن مجرم يرسل بريد إلكتـروني ليسأل عن معلومات تسجيل الدخول لمستخدم. فإذا أرسل المستخدم هذه المعلومات، فسوف تكون عديمة الفائدة بدون رمز العلامة. وحتى لو أرسل المستخدم إلى المهاجم كلمـة المـرور والرقم الحالي على شاشة العلامة، فإن هذا الرقم سوف يكون عديم الفائدة على الأغلب عندما يحاول المهاجم أن يستخدمه.

يمكن للمشتركين في الخدمة العريضة المجال المميـزة لأميركـا أونلايـن أن يشـتروا PassCode، وهو علامة SecurID يتم بيعها عبر AOL. يدخل المستخدمون رقم الرمز مع اسم المستخدم وكلمة المرور في كل مرة يسجلون الدخول إلى حسابهم AOL. وفي الوقـت الذي تم فيه نشر الكتاب، كانت AOL تفرض $9.95 من أجل العلامة بالإضافة إلى أجـرة شهرية $1.95. تقدم شركة السمسرة على الوب E*Trade أيضاً علامة إلى مستخدميها. وقد تقدم المصارف ومزودات الخدمة الأخرى عروض مشابهة في المستقبل.

على كل حال، مع أن العلامات الأمنية تقدم أمناً أكبر من كلمات المـرور البسـيطة، لكنها لديها مساوئها. تخيل أن كل مصرف، مزود خدمة ISP وشركة تجارة إلكترونية لديك أعمال معها، ستعطيك علامة. وفي كل مرة تريد إنجاز معاملة على الوب، يجب أن تبحث في درج مليء بالعلامات لكي تجد العلامة المناسبة. كما أن حياة بطارية العلامة محدودة، ويمكن أن تضيع العلامة، يتم سرقتها أو تتعرض للتلف.

وهناك مسألة على غاية الأهمية وهي ازدياد خبرة المهاجمين. فالتحقق من الصحة الثنائي لن يكون مفيداً إذا تواجد برنامج خبيث على كمبيوترك ينتظر حتى تبدأ بتسجيل الدخول. أو وجود مجرم يقيم موقع وب خادع يمرر معلوماتك (بما في ذلك الرمز من العلامة) إلى الموقـع الحقيقي ويسجل الدخول في مكانك. النتيجة واحدة: سوف يملـك المهـاجم الوصـول إلى حسابك خلال فترة الجلسة المقبولة ويمكنه تنفيذ معاملات. لقد اكتشف خبراء الأمن في عالم الشركات أن الاستراتيجية الأفضل هي الدفاع في العمق، مثل استخدام علامة بالإضـافة إلى حماية كمبيوترك باستخدام برمجيات الحماية.

SpoofStick

إنه برنامج صغير يدعى ملحق برنامج الاستعراض الذي يساعد على تحديد مواقع الوب المزيفة. ينشئ شريط أدوات جديد في برنامج الاستعراض يبين أي المواقع تتجول بها في الوقت الحالي. على سبيل المثال، إذا ذهبت إلى www.ebay.com، فإن شريط SpoofStick يعرض "أنت في ebay.com". وإذا ذهبت إلى موقع وب يتظاهر بأنه ebay، يعرض SpoofStick العنوان IP فقط (على سبيل المثال، يعرض "أنت في 192.1.2.3"). فإذا عرض SpoofStick عنوان IP بدلاً من اسم الميدان الفعلي، فمن المحتمل أنك تزور موقعاً غير تابع للمؤسسة التي يدعي أنه ينتمي إليها.

في اليوم ذاته الذي حمّلت فيه SpoofStick، تلقيت رسالة إلكترونية تخبرني بضرورة تحديث حسابي eBay. عرفت أن هذه الرسالة خدعة، لأنه ليس لدي حساب eBay، لكنني نقرت الارتباط الموجود في الرسالة لأختبر قدرة SpoofStick على تحديد هذا الموقع المزيف. وقد كشفه. مع العلم أن رسالة البريد الإلكتروني وموقع الوب الخادع على درجة عالية من تقنية التزوير، لكن لم يتم خداع SpoofStick. لقد عرض شريط أدوات برنامج الاستعراض "أنت في ..." وذكر العنوان IP. بعد أن حذفت الرسالة المزورة، ذهبت لأتجول في موقع الوب eBay الحقيقي، وفي كل صفحة تجولت إليها، عرض SpoofStick "أنت في eBay.com".

تم إنشاء SpoofStick بجهود فيل لبين رئيس CoreStreet، شركة حماية كمبيوترية. يمكنك أن تحمّله من أجل إنترنت إكسبلورر وموزيللا فايرفوكس من www.corestreet.com/spoofstick. يعرض لبين أيضاً مجلة طريفة (www.vastlyimportant.com) تستحق الاطلاع عليها.

3-2 استعادة الهوية المسروقة

على الرغم من اتخاذ الاحتياطات القصوى، ولكن من الممكن أن تسقط الضحية ويتم سرقة هويتها. (تذكر، حتى ولم تعطي معلومات حسابك، يمكن سرقتها من قواعد البيانات الحكومية أو قواعد بيانات الشركة أو حتى من محفظتك). وفق احصائيات لجنة التجارة الفيدرالية فإن ما يقارب 10 مليون شخص قد وقعوا ضحايا لسرقة الهوية في 2003.

يحتاج استعادة الهوية المسروقة إلى صبر ومثابرة. وينصح خبراء سرقة الهوية بأن توثق كل المعاملات مع مختلف الأعمال والوكالات التي تعمل معها، تحفظ نسخ عن جميع السجلات، وتتبع المحادثات الهاتفية وتبعث برسالة إلى الشركة التي تحاول أن تحل قضية سرقة الهوية معها. نذكر فيما يلي بعض الأعمال الأخرى التي يجب أن تنفذها:

- كتابة تقرير بالسرقة إلى المصرف أو مزود الخدمة الذي يقدم الحساب المسروق. إذا فتح شخص حساب جديد باسمك، اطلب إغلاق الحساب. واطلب استشارة خبير بالخـــداع على الإنترنت بدلاً من الحديث مع ممثل خدمة الزبائن. وإذا أساء شـــخص اســـتخدام حساب موجود، أرسل تقريراً بهذه العمليات غير المرخصة.
- اتصل مع وكالات الاعتماد الرئيسية (Experian، Equifax وTransUnion) لتصرح عن عملية خداع. في المرة الأولى التي تصرح فيها عـــن عمليـــة خـــداع إلى إحـــدى الوكالات، تمرر هذه الوكالة التصريح إلى الوكالتين الأخريين. يمنع التصريح عن عمليـــة خداع فتح أي حساب جديد باسمك. انظر إلى القسم التالي من أجل معلومات الاتصال.
- بلّغ عن العملية في قسم الشرطة المحلية. فقد تطلب المصارف وشركات بطاقات الاعتماد تقرير من الشرطة قبل أن يتصرفوا في مسألة سرقة الهوية، لذلك يجب أن تطلب نســـخة عن البلاغ.
- املأ شهادة خطية عن السرقة من لجنة التجارة الدولية (FTC). فإنها تساعدك في تحديـــد وتجميع المعلومات التي يحتمل أن تطلبها المؤسسة التي تتحرى عن سرقة الهويـــة. لكـــي تحصل على نسخة عنها اذهب إلى /www.consumer.gov/idtheft وانقر الارتباط ID Theft Affidavit.
- أرسل بلاغ عن الجريمة إلى FTC، التي تحتفظ بقاعدة بيانات بتقارير سرقة الهوية. ومع أن FTC لن تساعدك بإصلاح الأضرار، لكنها تشارك هذه التقارير مع أقســـام الشـــرطة، وكالات اعتماد المستهلكين والمؤسسة التي تم ارتكاب سرقة الهوية منها. وعندما ترســـل بلاغاً عن السرقة، تساعد هذه المؤسسات على تعلم المزيد عن سرقة الهوية وكيف يمكن منعها.

4-2 لائحة التدقيق

استخدم هذه اللائحة كدليل مرجعي سريع للمواد المغطاة في هذا الفصل.

ما يجب أن تفعله

- طلب نسخة مجانية من تقريـــر اعتمـــادك بشـــكل ســـنوي. يمكنـــك أن تـــذهب إلى www.annua/creditreport.com أو تتصل بالرقم 877-322-8228.
- تدقيق بيانات مصرفك وبطاقة اعتمادك بشكل دوري والبحث عن أي إشارة لنشاط غير عادي أو مشبوه.
- كن متشككاً بأي اتصال (سواء بالهاتف أو عبر البريد الإلكتروني) يسألك عن معلومات حساسة.

- استخدام برمجيات مضادة للفيروسات ومضادة للسبايوير لمنع برامج سرقة الهوية من غزو كمبيوترك.
- تمزيق المستندات الحساسة، بما في ذلك بيانات المصرف وبطاقة الاعتماد وعروض بطاقة الاعتماد، قبل رميها في سلة المهملات.
- إرسال بلاغ عن الخداع إلى وكالات تقرير الاعتماد الرئيسية الثلاثة إذا اشتبهت أو تأكدت من سرقة هويتك:

  Equifax,www.equifax.com,888-766-0008

  Experian,www.experian.com,888-397-3742

  TransUnion,www.transunion.com,800-680-7289
- إرسال تقرير للشرطة واملأ الشهادة الخطية عن السرقة إذا تم سرقة هويتك. يمكن أن تحصل على الشهادة الخطية عن السرقة ID Theft Addidavit من الموقع .www.consumer.gov/idtheft/

ما يجب أن لا تفعله

- الإجابة على البريد الإلكتروني الذي يسألك عن معلومات التعريف الشخصية أو أرقام الحسابات.
- نقر ارتباطات متضمنة في البريد الإلكتروني تدّعي أنها صادرة من مصرفك أو من شركة تجارة إلكترونية.
- فتح رسالة البريد الإلكتروني التي تدّعي أنها صادرة من مصارف أو من مواقع تجارة إلكترونية ليس لديك حسابات فيها.
- التصريح عن رقم الضمان الاجتماعي كمعرّف إذا لم تضطر إلى ذلك.

5-2 موارد مساعدة

يقدم هذا القسم موارد إضافية لمساعدتك على تعلم المزيد.

تقدم فيزا Visa بعض الملاحظات لحماية هويتك الرقمية وحمايتك من الخداع، كالخداع عبر الهاتف. اذهب إلى www.international.visa.com/ps/products/protect/main.jsp.

يمكن أن ترسل تقريراً بمحاولات التصيد إلى FTC على العنوان spam@vce.gor. ويمكنك أن ترسل بلاغاً إذا كنت تظن بأنك تعرضت لسرقة الهوية. اذهب إلى www.ftc.gov وانقر الارتباط File a complaint على الشريط الأزرق قرب أعلى الصفحة. ولكي تعرف المزيد عن الخطوات الأخرى التي يجب أن تتخذها إذا تعرضت لسرقة الهوية،

اذهب إلى www.consumer.gov/idtheft، وتديره FTC أيضاً. إنه يحتوي على معلومـــات مكثفة عن إرسال تقارير عن السرقة إلى وكالات الاعتماد وأقسام الشرطة. كمـــا يمكنـــك الاتصال بالخط الساخن لسرقة الهوية لدى FTC على الـــرقم 877-IDTHEFT (-877-438 4338) للحصول على معلومات وطلب النصيحة.

إذا تعرضت لسرقة الهوية، يمكن أن ترسل بلاغاً إلى مركز شكاوي جـــرائم الإنترنـــت (IC3,www.ic3.gov). إن IC3 هي مشروع مشترك بين FBI ومركز جرائم الطوق الأبيض الوطني. لاحظ أن إرسال شكوى لا يعني أن FBI سوف تعتمد شكواك. بل ســـوف يـــتم استخدام معلومات على الأغلب في البحث، لكن يمكن توجيه الشكوى إلى قسم شرطة محلي لتنفيذ الخطوات الإجرائية. يمكنك أن تجد ارتباط إلى الشكوى في الموقع www.ic3.gov.

إن مركز موارد سرقة الهوية هي مجموعة غير ربحية تقدم معلومات لمساعدة المستخدمين بمنع سرقة الهوية واستعادة الهوية المسروقة: www.idtheftcenter.org. ومثل FTC، يقـــدم هذا المركز معلومات مساعدة عن طريقة استعادة الهوية المسروقة. انقر علامة التبويب مـــوارد الضحية Victim's Resourcesعلى الجانب الأيسر من الصفحة.

ومجموعة العمل المضادة للتصيد (APWG) هي جمعية لرجال الأعمال، مزودات الخدمـــة، بائعي أجهزة أمن الكمبيوتر، وأقسام الشرطة. تتعقب APWG عمليات التصيد، وتحفظ سجلات برسائل البريد الإلكتروني المستخدمة في التصيد، تقدم توجيهات من أجل الممارســـات الأفضـــل لرجال الأعمال والمستخدمين لمنع والاستجابة لسرقة الهوية، وتقدم المواد التدريبيـــة. إذا ســـاورك الشك برسالة بريد إلكتروني، ابحث في سجلات التصيد. اذهـــب إلى www.anti-phishing.org وانقر الارتباط Phishing Archive على الجانب الأيسر من صفحة البدء. يمكنك أيضاً أن توجـــه رسائل التصيد إلى المجموعة على العنوان reportphishing@antiphishing.org.

إجبار الشركات على التصريح عن اختراقات الخصوصية

تم إصدار قانون جديد يدعى مذكرة مجلس الشيوخ في كاليفورنيا 1386 (SB 1386) في 1 تموز 2003. يفرض هذا القانون على الشركات التي تتعامل مع زبائن من كاليفورنيا على إعلامهم بعمليات كشف المعلومات الشخصية المعروفة أو المشتبهة إلى الأشـــخاص غـــير المرخصين. تعرّف مذكرة كاليفورنيا المعلومات الشخصية كالاســـم الأول للشـــخص أو الأحرف البادئة والكنية، مع أي مما يلي:

- رقم الضمان الاجتماعي.
- رقم شهادة القيادة.

- رقم الحساب، رقم بطاقة الاعتماد أو الاستدانة، بالإضافة إلى ما تسمح كلمة المرور أو الرمز الأمني به عند الوصول إلى الحساب.

تعرّف المذكرة أيضاً عدة أنواع من طرق الإعلام المقبولة:

- الإعلام المكتوب.
- الإعلام الإلكتروني.
- استبدال الإعلام إذا تجاوز كلفته 250000$ أو إذا كان يجب إعلام أكثر من 500000 شخص. تتضمن طرق الإعلام البديلة البريد الإلكتروني، الإعلان الواضح على صفحة وب المؤسسة أو الإعلان في أجهزة إعلام الولاية.

كما تصرح المذكرة أيضاً أن المؤسسات غير مجبورة بالكشف عن أي اختراق للمعلومات الشخصية إذا كان هذا الكشف سوف يؤثر على عمليات التحري الجارية.

إن هذه المذكرة مهمة لأنها تشكل دافعاً قانونياً لإرسال تقارير عن أي خرق للخصوصية، هذا الشيء الذي قد لا يحصل لولا ذلك لأن الشركات تعارض علناً التصريح عن عمليات التدخل المهمة. وتشجع هذه المذكرة الشركات أيضاً على العناية بشكل أفضل بالمعلومات الخاصة لكي توفر على نفسها الإحراج، فقدان رضا الزبائن، والدعاوى القضائية التي قد تنتج عن كشف غير المرخص للمعلومات.

إذا كنت من بين ملايين الأميركيين الذين لا يعيشون في كاليفورنيا، قد تقول، "من يهتم؟". حسناً، أحد الأسباب هي أن المذكرة تنطبق على الشركات التي تملك مواطنين في كاليفورنيا كزبائن، وليس فقط الشركات المتواجدة على أرض كاليفورنيا. لذلك سوف يتم إجبار الأعمال الجارية خارج كاليفورنيا على الأغلب بالتصريح عن كشف المعلومات الشخصية.

هناك حالة مهمة هي حادثة ChoicePoint. في شباط 2005، أعلنت شركة تجميع البيانات، التي تجمع المعلومات الشخصية مثل أرقام الضمان الاجتماعي وبطاقات الاعتماد لملايين من المستخدمين، أن المجرمين قد خدعوا الشركة وكشفوا عن معلومات الهوية الشخصية لآلاف من مواطني كاليفورنيا. لقد قامت ChoicePoint، التي يقع مقرها في جورجيا، بهذا الإعلان بسبب SB 1386. على كل حال، سأل المحققون بشكل علني المجرمين فيما إذا كانوا قد استهدفوا مواطني كاليفورنيا فقط، وسألت النيابة العامة لتسع عشرة ولاية لتعرف فيما إذا تم التوصل إلى معلومات مواطني الولايات الأخرى. وتحت الضغط اعترفت ChoicePoint أنه قد تم كشف المعلومات عن مستخدمين في ولايات أخرى أيضاً – أكثر من 145000 ملف مستخدم.

لقد تم اقتراح SB 1386 كنموذج لقانون فيدرالي يتم تطبيقه على البلاد بأكملـــها. تقدم بالاقتراح الفيدرالي سيناتور كاليفورنيا ديان فينشتاين، وهو معرف بالمذكرة بمجلـــس الشـــيوخ، S. 1350. يمكنـــك أن تقـــرأ نـــص التشـــريع المقتـــرح بالـــذهاب إلى http://thomas.loc.gov/home/search.html والبحث عن رقم المـــذكرة S. 1350 في جلسة الكونغرس 108.

تجربة شخصية مع سرقة الهوية

تلقيت رسالة في آذار 2005 من كلية بوسطن التي تخرجت منها. وليس كما في بريد المتخرجين العادي الذي يطلب تقديم المساعدة الحالية، وصفت هـــذه الرســـالة اختـــراق كمبيوتر يحتوي على معلومات شخصية – أسماء، عناوين؛ وأرقام الضـــمان الاجتمـــاعي، بطاقات الاعتماد والهواتف – لما يقارب 120000 متخرج، بما فيهم أنا.

حسب ما قالته الكلية، فإن المتدخل لم يدخل عنوةً لسرقة المعلومات الشخصية. وقد توصلت عمليات التحري في الكلية إلى أن المهاجم قام بقرصـــنة الكمبيـــوتر واســـتخدمه كمحطة ليهاجم أهداف أخرى.

بالإضافة إلى الرسالة التي أعلمتني عن الاختراق، بعثت الكلية ورقة وقائع مع تعليمات إرسال إعلام بالخداع إلى وكالات الاعتمـــاد الثلاثـــة الرئيســـية Equifax، Experian، وTransUnion. في البداية ظننت أن المعلومات آمنة، لأنني اعتقدت أن الكلية على حـــق بأن المهاجم لم يحاول أن يسرق أي بيانات. على كل حال، كنت قد أنهيت مؤخراً هـــذا الفصل عن سرقة الهوية، لذلك قررت أن المهاجم لن يـــؤذي المعلومـــات الموجـــودة في الكمبيوتر.

لقد اخترت Experian بشكل عشوائي من أجل الاتصال الأول. (يمكنك أن تجـــد الأرقام 800 لجميع مكاتب الاعتماد الثلاثة في القسم "لائحة تدقيق"). وتم إجراء كامـــل المعاملة عبر الموجه الصوتي المؤتمت؛ ولم أسمع خياراً للحديث مع إنسان. على كل حـــال، كان النظام المؤتمت سهلاً. وبعد طلب إضافة إعلام بالخداع مؤقت، اســـتخدمت لوحـــة الأزرار على هاتفي لإدخال رقم الضمان الاجتماعي ورمز المنطقة. واخترت أيضاً أن تتصل بي شركات بطاقات الاعتماد للتأكد قبل فتح أي حساب جديد باسمي (أدخلت رقم على هاتفي لإنجاز ذلك). فأعطاني النظام المؤتمت رقم تأكيد لأنك يجب أن تجهز قلم وورقة إذا أردت الخوض في ذلك)؛ أعطاني Experian أيضاً الخيار بمشاركة هـــذا الإعـــلام مـــع Equifax وTransUnion. قبلت هذا الخيار لأوفر على نفسي مكالمتين هاتفيتين إضافيتين وضغط المزيد من أزرار الهاتف. وبعد عدة أيام لاحقة تلقيت رسائل من وكالات الاعتماد الثلاثة تؤكد أنه تم الإعلام بالخداع.

أجريت اتصالاً آخراً لكي أطلب نسخة من تقرير اعتمادي. يمكنك أن تطلب تقرير الاعتماد من أي من وكالات الاعتماد الثلاثة. ويمكنك أن تذهب أيضاً إلى موقع خاص لكي تطلبه على الوب (www.annualcreditreport.com) أو يمكنك أن تتصل بالرقم 877-322-82228. ومرة ثانية توجب علي أن أتابع نظام صوتي مؤتمت. وقد كان هذا النظام أذكى قليلاً من نظام Experian لأنه طلب معلومات أكثر، بما في ذلك عنواني وتاريخ ولادتي. وقد أورد النظام أيضاً عنواني بشكل صحيح، فتطلّب تصحيحه قليلاً من العمل. يمكن أن يستجيب النظام إلى لوحة الأزرار أو إلى الأوامر الصوتية، لكنه احتاج إلى عدة محاولات لإدخال المعلومات بشكل صحيح.

ثم اتصلت بإدارة الأمن الاجتماعي (SSA)، على كل حال، لم يستطع الممثل الذي تحدثت معه أن يخبرني فيما إذا كان قد أساء شخص ما استخدام رقم الضمان الاجتماعي الخاص بي. واقترح أن اتخذ الخطوات المشروحة سابقاً. وقال أيضاً إذا قد تم استخدام رقم الضمان الاجتماعي الخاص بي بشكل سيء، يجب أن أرسل مستند الإساءة إلى فرع SSA المحلي، الذي يراجع المشكلة ليعرف فيما إذا كان إصدار رقم جديد مضموناً.

أما اتصالي الأخير فكان إلى قسم الشرطة المحلية. وشعرت بأنني غير متأكداً من ضرورة إجراء هذا الاتصال، لأنني كنت متأكداً من أنه لم يتم سرقة أي شيء، ولكنني قررت أنه لا مانع من إجراء الاتصال. استخدمت رقماً غير رقم الطوارئ، لكنه كان واضحاً على الفور أن سرقة الهوية ليست أفضلية لقسم الشرطة في أوكلاند. يصلك رقم غير الطوارئ إلى نظام صوتي مؤتمت آخر، ولا يوجد أي من الخيارات المقدمة بنظام الرسائل (تدقيق حالة الكفالة لشخص ما، تقرير عن جرم أحداث، وهكذا). أخيراً، وصلت إلى السكرتيرة الآلية لمكتب المقاطعة الجوال. تركت رسالة، ولكن لم أتلقى أي اتصال. (لا ألومهم لعدم الاتصال؛ وفوق ذلك لم يتم ارتكاب أي جريمة يمكنني التبليغ عنها).

يقول الخبراء أن الحصول على تقرير من الشرطة هو أمر أساسي لحل قضايا سرقة الهوية، لكنني سمعت أيضاً أن تحقيق شروط هذا الأمر صعب جداً لأن قسم الشرطة المحلية لا يعرف ما الذي يفعله بشأن هذا الطلب. أقترح عندما تحتاج إلى هذا التقرير أن تذهب إلى قسم الشرطة وتقابل الضابط شخصياً لتضمن أن تتحدث مع إنسان (نظام الهاتف المؤتمت هو جدار آخر). وبذلك يمكنك شرح أن التقرير ضروري من أجل شركة بطاقة الاعتماد أو المصرف، وتؤكد للضابط أنك لا تنتظر من قسم الشرطة المحلية أن يقوم بالتحقيق.

الفصل الثالث

جدران النار

جدار النار هو قطعة برمجية أو قطعة من العتاد تدير اتصـــالات الإنترنـــت إلى ومـــن كمبيوترك. dراقب جدار النار البرامج والتطبيقات التي تحاول أن تقيم اتصال مع كمبيوترك من الإنترنت، ويتحكم بالبرامج على كمبيوترك المسموح لها بإرسال المعلومات إلى الإنترنت.

لقد طلبت منك أمك على الأغلب أن لا تتكلم أبداً مع الغرباء، وهذا منطقي – يوجد الكثير من الناس الذين لا يمكن الوثوق بهم. وتظل نصيحتها سارية أيضاً على الإنترنت. فجدار النار المكون بشكل مناسب هو إصدار مبرمج من تعليمـــات أمـــك. إن الإنترنـــت مليئـــة بالكمبيوترات التي لا يمكنك الوثوق بها، وجدار النار يمنع كمبيوترك من الانخراط في حوار مع الغرباء. بكلمات أخرى، يمكنه منع الوصلات غير المطلوبة من كمبيوترك على الإنترنت. ولا يؤثر ذلك على الوصلات المطلوبة، كما عندما تبدأ برنامج الاستعراض وتكتب URL محدد في حقل العنوان أو عندما تدقق بريدك الإلكتروني. فتقيم الوصلة مع كمبيوتر آخر، ثم يشترك هذا الكمبيوتر في عملية تبادل المعلومات. إن الدور الرئيسي لجدار النار هو أن ينبهك عن محاولات الوصلات غير المرغوبة ويحجزها.

تشكل جدران النار حماية قوية من أنواع مختلفة من التهديدات، كما في حالة المهاجمين الذين يمسحون الإنترنت بحثاً عن الضحايا المهمين، والديدان المؤتمتة. كما تعلمت في الفصـــل الأول، "فهم مخاطر الإنترنت"، الديدان هي برامج تحاول استغلال نقاط الخلل البرمجي للوصول إلى الكمبيوترات والتحكم بأكبر قدر منها. وجدران النار فعالة في كشف هذه الأنواع مـــن الديدان التي تعتمد على الوصلات غير المطلوبة، حيث يحاول كمبيوتر لم تتصل به أن يصل إلى كمبيوترك.

يتعمق القسم التالي قليلاً في الطريقة التي يتحدث بها كمبيوترك مع الكمبيوترات الأخرى على الإنترنت. فيسمح ذلك بفهم طريقة عمل جدار النار بشكل أفضل، ولماذا هو أداة قيّمة لأي شخص يستخدم الإنترنت. تختبر الأقسام التالية جداري نار، يمكنك الحصـــول عليهمـــا

مجاناً، وبالإضافة إلى ذلك تتحدث عن دواعي تكبد الكلفة الضرورية لحماية البرمجيات. ويركز هذا الفصل بشكل خاص على جدران النار البرمجية (أي جدران النار التي يتم تثبيتها على قرصك الصلب كأي تطبيق برمجي آخر). أما عتاد جدران النار فينجز الوظائف نفسها ولكن مع جهاز منفصل يوجد بين كمبيوترك ووصلة الإنترنت. ويستخدم جدار النار في العديد من الموجهات التي تسمح بتشارك عدة كمبيوترات بوصلة إنترنت واحدة.

1-3 الرزم، البروتوكولات، والمنافذ

كلما تعلمت عن الإنترنت أكثر، ازددت دهشةً من كونها تعمل حقاً. لقد بذلت العديد من العقول اللامعة قصارى جهدها لإخفاء تعقيد الإنترنت خلف تطبيقات سهلة الاستخدام. يجرد هذا القسم طبقة أو اثنتين من واجهتها لكي تقدر عمل الإنترنت بشكل أفضل وتعرف ضرورة استخدام برمجيات تحكمية مثل جدار النار. أما إذا لم يكن لديك فضول نهائياً حول طريقة عمل الإنترنت، يمكنك تجاوز القسم التالي، ولكنك إذا قرأته ستكون على الأقل قادراً على الحديث أمام زملائك عن دعامات الإنترنت التقنية.

تدعى الوحدة الأساسية في اتصالات الإنترنت الرزمة. وتتألف كل صفحة وب تراها، رسالة إلكترونية تتلقاها أو ملف تحمّله من رزم صغيرة، ويتم تسليم كل منها بشكل منفرد إلى كمبيوترك. ثم يعيد الكمبيوتر تجميع هذه الرزم في بنية متماسكة ويعرضها عليك.

تخضع طريقة بناء الرزم، عنونتها وتوجيهها عبر الإنترنت إلى مجموعة من القواعد التي تقدم إطار عمل لكل كمبيوتر. تدعى هذه القواعد بروتوكولات. ويتم مراقبتها من عدة مؤسسات، مثل قوة مهام هندسة الإنترنت (IETF,www.ietf.org) وIEEE (معهد مهندسي الكهرباء والإلكترون، www.ieee.org).

تستخدم البروتوكولات والتطبيقات المنافذ لكي تصل إلى الكمبيوترات المنفردة. والمنافذ هي الطرق التي تدخل المعلومات منها إلى الكمبيوتر وتغادره. يوجد 65535 منفذاً مستخدماً في الوقت الحالي، وتستخدم بعض التقنيات منافذ خاصة. على سبيل المثال، يستخدم البروتوكول HTTP (الوب) المنفذين 80 و8080، أما البروتوكول HTTPS (بيانات الوب المشفرة) فيستخدم المنفذ 443. وتستخدم برامج مشاركة الملفات وأنظمة الرسائل الفورية منافذ مختلفة؛ كما تستخدم العديد من هذه البرامج أي منفذ غير مشغول.

بما أن التطبيقات تستخدم المنافذ للوصول إلى الكمبيوترات، فأحد وظائف جدار النار هو مراقبة أي المنافذ مرخص لها بالاتصال مع الكمبيوتر.والمنافذ هي كينونات منطقية وليست

فيزيائية، لذلك لا تكلف نفسك عناء البحث عن 65535 مأخذ صغير على الواجهة الخلفية لكمبيوترك.

IP و TCP

البروتوكولان الأساسيان في الإنترنت هما IP (بروتوكول إنترنت) وTCP (بروتوكول التحكم بالإرسال). ربما سمعت IP من خلال (VoIP) الصوت عبر IP، تقنية جديدة تسمح بإجراء الاتصالات الهاتفية عبر الإنترنت.

يصف البروتوكول IP طريقة إرسال الرزم من كمبيوتر إلى آخر، وكل كمبيوتر على الإنترنت يملك عنواناً (عنوان IP). يتشكل هذا العنوان من أربع مجموعات حتى ثلاثة أرقام، كل منها مفصول بنقطة. وهذا مثال عن العنوان IP: 192.101.432.156.

إذا كنت تستخدم مودم اتصال هاتفي من أجل الوصول إلى الإنترنت، فإن مزود الخدمة يسند عنوان IP جديد إلى كمبيوترك في كل مرة تصل فيها إلى الإنترنت. ويحدث الشيء نفسه مع مودمات الكابل والوصلات DSL (خط المشترك الرقمي)، ما عدا أن العنوان IP يبقى معك طالما أن لم تسجل الخروج أو تغلق كمبيوترك. فالعديد من الناس الذين يستخدمون مودمات الكابل والوصلات DSL يتركون الإنترنت موصولة لأيام أو أسابيع متواصلة.

ومع أنه أمر جيد أن تملك وصول لحظي إلى الإنترنت، لكن العنوان IP طويل الأمد يشكل خطراً. وذلك لأن مجرمي الكمبيوتر يمسحون الإنترنت بشكل مستمر باستخدام برمجيات خاصة تبحث عن الكمبيوترات سهلة الاختراق. يستغرق مسح أعداد كبيرة من أجهزة الإنترنت زمناً، وهذه الأدوات تؤشر على العناوين IP الضعيفة فيمكن أن يعود المجرم إليها لاحقاً. إذا كان العنوان IP الذي تستخدمه دائماً، فإن المجرم سوف يعثر عليك بسهولة مرة أخرى. على سبيل المثال، استخدم مبرمج الدودة Blaster.B أجهزة مصابة سابقاً كمحطات أوامر وسخرها في عدد من عمليات الهجوم الجديدة. وقد عرف أن هذه الأجهزة سوف تبقى متوفرة لأسابيع بعد اختراقها لأنها كانت موصولة عبر مودمات الكابل، لذلك بقيت العناوين IP نفسها. (الوصلات عالية السرعة مرغوبة أيضاً لمجرمي الإنترنت لأنها تمكنهم من شن الهجوم بسرعة أكبر من وصلات الاتصال الهاتفي).

يجب أن يملك كل مستخدم على الإنترنت جدار نار لأن كل مستخدم على الإنترنت يملك عنوان – تشبه مسألة وضع قفل على الباب. في الوقت الحالي يوجد على الإنترنت الكثير من الأبواب غير الموصدة، لذلك يختار المجرمون من بينها أهدافهم. وباستخدام جدار نار تم إعداده بشكل جيد، تنتشل نفسك من بركة الأهداف السهلة. ويوضح ذلك نقطة مهمة حول أمن الكمبيوتر. لست مضطراً لأن يكون نظامك الأمني أمثلياً – بل يجب أن يكون أفضل مما

لدى جيرانك فقط. إذا أقفلت بابك في الليل وجيرانك أبوابهم غير مقفلة، فإن المجرم الــذكي سوف يذهب إلى الأهداف الأسهل.

كما ذكرنا سابقاً، عندما يرسل كمبيوتر المعلومات إلى كمبيوتر آخر فإنه يقسم هــذه المعلومات إلى رزم. ويتم ختم كل رزمة بالعنوان IP للكمبيوتر (عنوان المصدر) والعنوان IP للمستلم (عنوان الوجهة). تحتوي كل رزمة على جزء من المعلومات الكلية التي يجب إرسالها إلى الوجهة (يدعى هذا القسم من المعلومات بالحمولة payload). ويبعث المرسل رزمــه إلى موجه محلي. أما الموجه فهو كمبيوتر شبكة مهمته تمرير الرزم من مكان إلى آخــر. وتحــتفظ الموجهات بسجلات تدعى جداول تصف المسارات الأفضل إلى الوجهات المختلفــة علــى الشبكة. ويمكن أن تسافر الرزم عبر عدة موجهات قبل أن تصل إلى الكمبيوتر المستلم.

يدعى البروتوكول IP ببروتوكول "الجهد الأفضل". ولا يملك هذا البروتوكول أي آلية لتحديد فيما إذا كانت الرزم قد وصلت إلى وجهتها. فالبروتوكول IP يقذف رزمه ببســاطة في الشبكة ويأمل في أنها ستفلح بالوصول إلى وجهتها.

لقد تم تطوير TCP من أجل إضافة مزيداً من التحكم إلى الرسائل المرسلة والمســتقبلة. لذلك يضيف TCP أرقام متابعة إلى الإرسال فيعرف الكمبيوتر المستلم عدد الرزم التي يتوقع وصولها (على سبيل المثال، هذه هي الرزمة رقم 5 من أصل ثمانية رزم). ويقدم TCP أيضاً آلية لضمان وصول جميع الرزم المرسلة، وإذا لم تصل جميعها، يتم إعادة إرسال الــرزم المفقــودة. وحسب قرارات التوجيه خلال الرحلة قد تصل الرزمة 5 قبل الرزمة 4. فيحتفظ الكمبيــوتر المستلم بالرزم حتى تصل جميعها ثم يعيد تجميعها حسب الترتيب الصحيح ويمررها إلى الطبقات الأخرى في الكمبيوتر لمتابعة المعالجة.

يدعى البروتوكول TCP بروتوكول حالة لأنه يراقب حالة الإرسال. وبدلاً من قذف الرزم في الإنترنت فقط، يتصل TCP بالكمبيوتر المرسل ويراقب الإرسال لكي يتأكد من وصول جميــع الرزم. وإذا لم يتحقق ذلك، يمكن أن يطلب الكمبيوتر المستلم إعادة إرسال الرزم المفقودة.

HTTP و HTML

هذان البروتوكولان ليسا بروتوكولي إنترنت تقنياً. إنهما بروتوكولا شبكة الوب العالمية. ومع أن العديد من الناس يستخدمون الوب والإنترنت بشكل متبادل، ولكنــهما كينونتــان منفصلتان. ما هو الفرق بينهما؟ الإنترنت هي آلية لوصل الكمبيوترات عبر مسافة فيزيائية. أما شبكة الوب العالمية فهي طريقة منظمة لعرض المعلومات والتحول عبر مستودعات المعلومات (مثل مواقع الوب). فالوب يعمل على الإنترنت؛ أي أن البروتوكولات المستخدمة في الــوب يتم نقلها من مكان إلى آخر باستخدام بروتوكولات مثل TCP وIP.

اخترع بيرنرزلي، فيزيائي بريطاني، شبكة الوب العالمية بإنشاء لغة ترميز النصوص الفائقة

(HTML) وبروتوكول نقل النصوص الفائقة (HTTP)، واللغة HTML هي المعتمدة لإنشاء صفحات الوب. أما HTTP فهو آلية لنقل HTML.

ترشد HTML برامج استعراض الوب حول طريقة عرض النصوص وتعطي المستخدمين القدرة على نقر ارتباطات متضمنة في النص. يمكنك أن تشاهد شيفرة المصدر HTML على صفحة وب في برنامج الاستعراض إنترنت إكسبلورر بفتح القائمة View في أعلى الصفحة واختيار Source.

كانت المساهمة المميزة لبيرنرزلي هي السماح باستخدام فكرته لأي شخص يرغب بذلك، فأدى هذا الأمر إلى ازدهار إبداعه ونشوء الوب كوسط غني بالمعلومات يتم النفاذ إليه بسهولة.

وكان تطوير برنامج استعراض الوب نيتسكيب نافيغيتر المساهمة المهمة الأخرى في تطوير شبكة الوب العالمية. كتبه مارك أندريسين وجيم كلارك، وقد أنشأ بيئة مشتركة لعرض صفحات الوب. وفي هذا اليوم أصبحت برامج الاستعراض الوسيلة الأوسع استخداماً التي يطل منها الناس على شبكة الوب العالمية والإنترنت.

2-3 ما الذي يمكن أن تفعله جدران النار

لقد بدأنا هذا الفصل بمقارنة جدران النار مع نصيحة الأم بعدم الحديث مع الغرباء. أما الآن فسوف نتحدث المزيد عن الطريقة التي تتبعها جدران النار في حماية نفسها، بالإضافة إلى اختبار محدوديتها.

تنظيم الوصلات الواردة والصادرة

الوظيفة الرئيسية لجدار النار هي تنظيم الوصلات الواردة والصادرة من كمبيوترك. ويؤدي هذه المهمة باختبار كل تطبيق أو بروتوكول يحاول أن يفتح منفذ على كمبيوترك. قد لا تكون على دراية بذلك، ولكن عندما تكون على الإنترنت تنقر البرامج بابك بشكل مستمر. فإذا كان لديك جدار نار مثبتاً، يمكنك إعداده لينبهك في كل مرة يحول أي برنامج أن يقيم وصلة مع كمبيوترك. وغالباً ما تكون هذه البرامج ماسحات منافذ، وهي أدوات برمجية تمسح الأجهزة وتبحث عن منافذ مفتوحة يمكن استخدامها للوصول إلى الكمبيوتر.

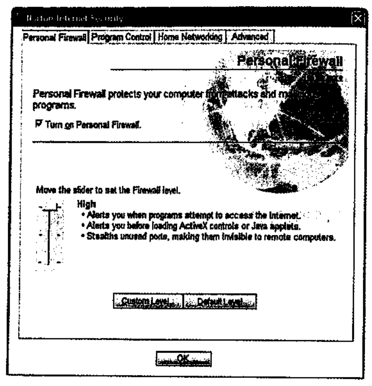
ومن المهم أيضاً أن يكون جدار النار قادراً على اعتراض حوار كمبيوترك مع الإنترنت. فإذا كان لديك على الكمبيوتر حصان طروادة، سبايوير أو أي نوع آخر من مالوير، يمكن لجدار النار أن يمنعه من إقامة وصلات صادرة إلى الكمبيوترات الأخرى. وهذا الأمر ضروري لأنه يمنع كمبيوترك من أن يصبح مصدراً لبدء عمليات الهجوم على الكمبيوترات الأخرى، أن يسمح لسبايوير بإرسال تقارير عن نشاطاتك أو أن يسمح لمالوير بتلقي أوامر جديدة أو يتم ترقيتها من نظام تحكم.

يجب أن يكون جدار النار الجيد قادراً على أداء ما يلي:

- يجعل كمبيوترك غير مرئي. تذكر أن كمبيوتر يملك 65535 منفذ، يمكن استخدام كل منها لتمهيد وصلة مع كمبيوتر آخر على الإنترنت. ومع أنه أمر هام أن تسمح لكمبيوترك باستخدام المنافذ المرتبطة مع التطبيقات الشائعة مثل الوب، البريد الإلكتروني، والرسائل الفورية، لكن لا يوجد داعٍ لأن تحاول الكمبيوترات غير المعروفة على الإنترنت أن تصل إلى كمبيوترك عبر المنافذ غير المستخدمة بشكل عام. فإحدى الطرق التي يصل فيها المجرمون إلى الكمبيوترات تتم بمحاولة فتح وصلات على كل منفذ محتمل على النظام الهدف. ينجزون ذلك بإرسال طلبات TCP/IP، فإذا استجاب الكمبيوتر الهدف إلى طلب محدد، يكون المجرم قد وجد مدخل مهم إلى كمبيوترك. كذلك، لا يستجيب جدار النار الجيد إلى طلبات TCP/IP إلى المنافذ غير المستخدمة في وظائف الإنترنت العامة. فعندما لا يستجيب كمبيوترك يصبح غير مرئياً بالفعل. ويدعى ذلك غالباً بوضع الكمبيوتر في نمط الصمت.
- ينبهك عن السلوك المشبوه. يجب أن يكون جدار النار قادراً على إخبارك عندما يحاول برنامج أو وصلة أن ينفذ شيء غير مرغوب، مثل تحميل البرمجيات أو تشغيل برنامج مثل أكتيف إكس (أكتيف إكس هي تقنية من مايكروسوفت يمكنها أن تنفذ البرامج المحملة في إنترنت إكسبلورر). إن بعض برامج أكتيف إكس جيدة، لكن المجرمين يستغلون أكتيف إكس لإدخال مالوير على كمبيوترات المستخدمين. يمكنك أن تتعلم المزيد عن أكتيف إكس في الفصل الخامس، "التخلص من الضيوف غير المرغوبين"، الجزء 2: سبايوير، أدوير وأحصنة طروادة". على كل حال، تملك هذه الميزات سيئات أيضاً. فمع أنني أستجيب لطلبات الوصلات من مواقع الوب الموثوقة باطمئنان، ولكن العديد من رسائل التحذير صعبة الفهم. وبعض جدران النار مثل Zone Alarm Pro، يمكن أن تقدم معلومات إضافية عن التحذيرات لمساعدتك باتخاذ القرار والسماح بإنجاز عملية أو إقامة وصلة.
- يحجز الوصلات الصادرة التي لم تبدأها. كما ذكرنا، قد تحاول مالوير على كمبيوترك الاتصال بالكمبيوترات الأخرى على الإنترنت. فإذا لم تبدأ تشغيل برنامجاً بشكل صريح، فإن جدار النار الجيد سوف يخبرك عندما يحاول برنامج على كمبيوترك بالوصول إلى الإنترنت لوحده.

الإعدادات الأمنية

تسمح معظم جدران النار بضبط إعداداتها الأمنية. على سبيل المثال، تتضمن وحدة أمن الإنترنت في نورتون زالقة مع ثلاثة مستويات منخفض، متوسط ومرتفع، كما هو مبين في الشكل 3-1. تضبط هذه الإعدادات المستوى الأمني الذي يقدمه جدار النار. بشكل عام، عندما يكون الإعداد على مستوى أعلى تكون الحماية أكبر.



الشكل (3-1): إعدادات جدار النار لوحدة أمن الإنترنت في نورتون.

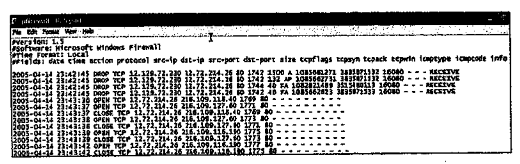
على كل حال، يقاطع إعداد المستوى المرتفع استخدام الإنترنت. فجدران النار الحذرة جداً قد تقاطع تجولك في الإنترنت وتقاطع تحميل الملفات والعمليات الأخرى التي تظن بأنها عادية لكن جدار النار يسيء الظن بها. فيكلفك ذلك مزيداً من الوقت لنقر الزر Allow من أجل متابعة العملية التي تم مقاطعتها.

إحدى الطرق لاختيار المستوى الأفضل بالنسبة إليك هي أن تبدأ بالمستوى الأعلى وترى حجم المقاطعة التي يسببها. ثم تزيح المؤشر نحو الأسفل بشكل متدرج حتى تصل إلى المستوى المناسب. تذكر دوماً عملية المقايضة: يسهّل المستوى الأمني المنخفض استخدام الإنترنت بشكل عام ولكنه يزيد من التعرض للهجوم. لذلك يجب أن تصل إلى التوازن الذي يناسبك.

قد يرغب المستخدمون المتقدمون بالعمل مع إعدادات جدار النار الداخلية وعدم الاقتصار على زلق الزالقة من المستوى المرتفع إلى المنخفض، كحجز منافذ أو تطبيقات محددة.

يتعقب جدار النار أيضاً جميع الكمبيوترات التي يتصل معها. تدعى هذه اللائحة سجل جدار النار. ولا يعنيك هذا السجل كثيراً ما لم يكن لديك بعض الخبرة في شبكات الكمبيوتر. لكن إذا كنت مهتماً بالتعرف على العنوان IP، المنافذ التي يستخدمها الكمبيوتر، والعناوين IP للأماكن التي تتصل معها، يجب عندئذ أن تنظر إلى السجل. يضم Windows XP Service Pack 2 جدار نار مبيت. ويستخدم ملف وجهة افتراضي للسجلات في الموقع

C:WINDOWS/pfirewall، كما هو مبين في الشكل 3-2، ومن الممكن وضع هذا الملف في أي مكان آخر. لاحظ أن وظيفة السجل تعمل من أجل جدار نار ويندوز. أمـــا منتجـــات جدران النار الأخرى فتنشئ سجلاتها الخاصة، ويمكنك العثور عليها عبر واجهة المستخدم.



الشكل (3-2): سجل جدار النار.

يضم تنسيق السجل تاريخ ووقت كل عملية، وصف العملية (على سبيل المثال، إقامـــة وصلة إلى كمبيوتر آخر)، البروتوكول (TCP وهكذا)، عنواني المصدر والوجهة IP، منفذي الوجهة والمصدر، ومعلومات الرزم المنفردة والتي تشكل الاتصالات عبر الإنترنت.

3-3 ما الذي لا يمكن لجدار النار أن يفعله

جدران النار هي مكون مهم في الأمن المنـــزلي، لكن لديها بعض الحدود. فالعديد من عمليات الهجوم على الإنترنت تستخدم المنافذ والتطبيقات المسموح بمرورها بشكل عام عـــبر جدار النار، بما في ذلك الوب والبريد الإلكتروني (وإذا لم يكن ذلك مســـموحاً فـــلا معـــنى لوجودك على الإنترنت)، ولن يوقف جدار النار على الأغلب عمليات الهجوم التي تســـتخدم هذه المداخل.

على سبيل المثال، أكثر طرق الإصابة شيوعاً بالفيروسات والديـــدان هـــي باســـتخدام ارتباطات البريد الإلكتروني. وطالما جدار النار يسمح بمرور البريد الإلكتروني، لا أمل بإيقاف الفيروسات التي تصل مع ارتباطات البريد الإلكتروني.

وينطبق الأمر نفسه على الوب. فالعديد من صفحات الوب تستخدم مختلف البرمجيات، مثل الكعكات، أكتيف إكس وجافا لجعل عملية الاستعراض أكثر سرعة وجاذبية. على كـــل حـــال، يمكن للمهاجمين استخدام جميع هذه البرامج بشكل سيء وتضمين مالوير في مواقع الوب. وتحمّـــل مالوير نفسها على كمبيوترك عندما تتجول في هذا الموقع (يدعى تحميل بالتجول).

أخيراً، تلتزم جدران النار بتنفيذ ما تقوله لها. فإذا سألك جدار النار عن السماح بتشغيل برنامج وأجبته بنعم، وإذا تبين أن هذا البرنامج خبيث، لا يمكنك أن تلوم جدار النـــار علـــى ذلك. فاتخاذ القرار بالسماح بإقامة وصلة هو أحد أكثر الأجزاء صعوبة في أمـــن الكمبيـــوتر للمستخدمين المنـــزليين.

توجد طريقتان للتعامل مع التنبيهات التي لا تفهمها. إذا كنت في موقع ذي سمعة طيبة، مثل موقع تجارة إلكترونية، ISP أو موقع مصرف تجاري معروف، يمكنك على الأغلب أن تسمح بتنفيذ البرامج بدون القلق كثيراً. على سبيل المثال، كلما أرسل ملف مرتبط مع رسالة البريد الإلكتروني باستخدام Yahoo! Mail، ينبهني جدار النار عن وجود برنامج أكتيف إكس. وأنقر دوماً الزر Allow لأنني أثق بالموقع !Yahoo. وإذا أردت توخي المزيد من الحرص، يوجد خيار آخر وهو منع تنفيذ العملية. فتجازف بأنه قد لا يتم تنفيذ التطبيق أو المعاملة، وفي هذه الحالة يجب أن تبدأ من جديد.

يوجد خيار آخر وهو أن تنسخ اسم البرنامج، التطبيق أو الخدمة التي تحاول إقامة وصلة ثم تلصقه في حقل البحث في محرك البحث المفضل لديك. قد تساعدك النتائج باتخاذ القرار حول السماح بإقامة الوصلة.

من أجل تحقيق حماية كاملة، يجب أن يتم استخدام برمجيات جدار النار بالاشتراك مع البرمجيات المضادة للفيروسات (AV) والبرمجيات المضادة للسبايوير، ويتم تغطية كليهما في هذا الكتاب.

4-3 جدران النار المجانية

إن الميزانية المحدودة ليست عذراً لقبول مستوى أمني ضعيف في الكمبيوتر. يبحث هذا القسم بجداري نار يمكنك أن تحمّلهما بدون كلفة. وهما من أفضل جدران النار المعروفة، ويسرد الجدول 3-2 جدران نار مجانية أخرى.

ويندوز XP سرفيس باك 2

تم معاقبة شركة مايكروسوفت بنجاحها. فقد أنتجت نظام تشغيل الكمبيوتر الأكثر انتشاراً في العالم، ويتم استهدافها بأوسع شكل من مجرمي الإنترنت. يكتشف مبرمجو مالوير وبرامج القرصنة الخبيثة بشكل دائم نقاط خلل في نظام تشغيل ويندوز وتطبيقات مايكروسوفت الأخرى ويستغلون هذا الخلل لقرصنة الكمبيوترات، سرقة أو تخريب البيانات، وارتكاب جرائم الإنترنت.

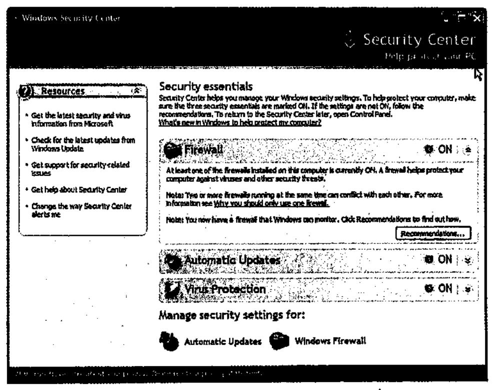
لقد هاجمت معظم الفيروسات والديدان المعروفة جيداً في السنوات القليلة الماضية (Blaster، Slammer، MyDoom، Code Red، Nimda، إلى آخره) ويندوز، إنترنت إكسبلورر أو تطبيقات مايكروسوفت الأخرى. ومع أنه يظن البعض أن أي دعاية هي أمر جيد، لكن الاستغلال المتكرر لمنتجات مايكروسوفت أدى إلى توجيه انتقادات لاذعة للشركة وجعل الكثير من الشركات تفضل خيارات أخرى مثل Linux. (يجب على المستخدمين أن يختاروا Mac لأنها تواجه قضايا أمنية أقل. وبالطبع إذا حصلت Mac على شهرة كمبيوترات

ويندوز، فإنني أضمن أن مجرمي الإنترنت سوف يجدون طرقاً لاستغلالها. على كل حال، منصة العمل Mac هي الأفضل للمستخدمين).

حاولت مايكروسوفت كتابة شيفرة أكثر أمناً وضمنت مزايا الأمن في منتجاتها. وخطوتها الأكبر نحو بيئة أكثر أمناً على جانب المستخدم هي ويندوز XP سيرفيس باك (SP2)، الترقية الأحدث لنظام تشغيل مايكروسوفت. الترقية SP2 متوفرة مجاناً (بافتراض أنك اشتريت XP – أما المستخدمين الذين يشغلون ويندوز 98، ويندوز 2000، ويندوز Me أو ويندوز 95 فحظهم سيء).

يمكنك أن تحمّل SP2 من Windows Update (لكنه ملف كبير، لذلك استعد للجلوس جانباً نصف ساعة على الأقل إذا كنت تستخدم وصلة اتصال هاتفي) أو يمكنك أن تطلب الترقية على قرص مضغوط من www.microsoft.com/windowsxp/sp2/default.mspx.

تتضمن SP2 مركز أمن ويندوز، المبين في الشكل 3-3، والذي يراقب المعلومات الأمنية الأساسية حول الكمبيوتر. ويستخدم رموز محجوبة بسيطة بالأخضر، الأصفر والأحمر للإشارة إلى حالة الكمبيوتر الأمنية. وبعد أن تثبت البرمجيات، يمكنك أن تجد مركز الأمن بفتح Control Panel، Security Center وتتحكم بمزايا SP2 الأمنية الثلاثة: Windows Firewall، Automatic Updates وVirus Protection.



الشكل (3-3): مركز أمن ويندوز.

جدار نار ويندوز

تتضمن SP2 برمجيات جدار نار مجانية مصممة خصيصاً لويندوز XP. وتمنع محـاولات إقامة الوصلة الواردة غير المطلوبة من الكمبيوترات أو البرامج الموجـودة علـى الإنترنـت. فالديدان، الفيروسات والمجرمين يحاولون الوصول إلى جدار النار باستخدام مختلـف المنافـذ والبروتوكولات. يمكن أن يحجز جدار نار ويندوز هذه المحاولات. على كل حال، كما مـع معظم جدران النار، يجب أن تخبر جدار نار ويندوز أي الوصلات تريد أن تقبلها وأي منـها تريد أن تحجزها. عندما تنقر Yes لكي تسمح بإقامة وصلة، تكون قد وضعت استثناءاً على قواعد جدار النار؛ فبعد أن تضع استثناء، لن يحجز جدار النار أي برامج مستقبلية على لائحة الاستثناءات.

تحتاج بعض البرامج إلى استثناءات لكي تعمل بشكل صحيح؛ على سبيل المثال، تستخدم الرسائل الفورية، مشاركة الملفات، والألعاب على الوب منافذ مختلفة. على كل حال، بازدياد عدد الاستثناءات يزداد عدد المنافذ التي تظل مفتوحة. كما ذكرنا، يمسح مجرمـو الإنترنـت الشبكة باستمرار بحثاً عن المنافذ المفتوحة التي تسمح لهم بالاتصال بكمبيوترك. لذلك من المفيد تحديد عدد الاستثناءات.

يتضمن جدار نار ويندوز سجل أيضاً. يسجل هذا السجل جميع نشاطات جدار النار بما في ذلك الوصلات المحجوزة والمسموحة. ولا تحتاج إلى مراقبة هذه السجلات، لكنها تقـدم معلومات قيّمة إذا لاحظت أن برامج معينة تتصرف بشكل غريـب أو إذا اشـتبهت بـأن كمبيوترك قد يكون مصاباً بمالوير.

يجب أن تؤهل هذا السجل بشكل صريح، لأنه غير مؤهل بشكل افتراضي. لكي تنفـذ ذلك، افتح جدار نار ويندوز وانقر علامة التبويب Advanced. وتحت لائحـة التسـجيل الأمني، يمكنك تحديد أحد خيارين: تسجيل الرزم المهملة، الذي يسرد جميع محاولات إقامـة الوصلة التي حجزها جدار النار أو تسجيل الوصلات الناجحة، الذي يذكر جميع الوصـلات التي سمح جدار النار بها.

إن كون جدار النار مجاني خطوة جيدة، لكن جدار النار SP2 يحمي فقط من الوصلات الواردة غير المرخصة. فالوصلات الواردة غير المطلوبة هي الأكثر خطراً، وجدار نار وينـدوز يؤدي نصف العمل فقط، لأنه لا يوقف مالوير الموجودة على كمبيوترك من إجراء الوصلات الصادرة. وهكذا فقد ترغب بالنظر إلى حلول بديلة. تراقب معظم جدران النـار التجاريـة (وجدار النار ZoneAlarm المجاني الذي يتم شرحه لاحقاً) الوصلات الـواردة والصـادرة. وبالتالي إذا كنت لا تريد شراء أو تحميل جدار نار آخر، فعلى الأقل يجب أن تستفيد من جدار نار ويندوز.

إذا كان لديك جدار نار آخر مثبتاً أو إذا كنت تفضل استخدام جدار نار مختلف، لــن تكون محمياً بشكل مضاعف باستخدام جدار نار آخر في الوقت نفسه مع جدار نار ويندوز. وبالفعل فإن تشغيل جداري نار أو أكثر على الكمبيوتر نفسه في الوقت نفسه قــد يقــاطع استخدام الإنترنت. لكي تلغي تأهيل جدار النار، انقر رمز جدار نار ويندوز في أسفل صفحة مركز الأمن. فتظهر نافذة منبثقة؛ انقر ببساطة الزر Off. ويمكن أن تلغي جدران النار الأخرى خلال عملية التثبيت حالة جدار نار ويندوز المؤهلة.

للحصول على لائحة الأسئلة المتكررة (FAQ) حول استخدام جدار نــار الإنترنــت لمايكروســـوفت، اذهـــب إلى /www.microsoft.com/athome/security/protect .firewall.mspx

لمزيد من المعلومات عن إعداد جدار نار ويندوز، انظر إلى الفصــل الســابع، "تــأمين ويندوز".

عمليات التحديث التلقائية

يكشف القراصنة باستمرار عن نقاط خلل جديدة في أنظمة الكمبيوتر، وخصوصــاً في منتجات مايكروسوفت، وفي كل مرة يتم فيها العثور على نقطــة خلــل جديــدة، تنشــئ مايكروسوفت رقعة تثبيت لمنع استغلال هذا الخلل باستخدام دودة أو فــيروس. وإذا أهّلــت عمليات التحديث التلقائية Automatic Updates، فإن مايكروسوفت ترسل هذه الرقع إلى كمبيوترك عند توفرها. لذلك يوصى بشدة باستخدام عمليات التحديث التلقائية نظراً للسرعة التي يتم فيها استغلال نقاط الخلل. إذا كنت غير مجتهداً على تحميل رقم نظــام التشــغيل أو تحديث البرمجيات AV، فإن الميزة Automatic Updates تقفل الطريق في وجه المستخدمين المسيئين بدون أن تبذل أي مجهود مميز. يناقش الفصل السابع الرقع والحلول.

الحماية من الفيروسات

لا يحميك SP2 من الفيروسات، لكنه يراقب حالة البرمجيات AV الأخرى. تخبرك الميزة Virus Protection فيما إذا كانت البرمجيات AV مؤهلة وفيما إذا كانت حديثة. وبــالطبع يجب أن يكون البرنامج AV قادراً على تنبيهك إذا أصبح قديماً، لكن لا يضر تذكيرك مــرة أخرى.

لا تدعم مايكروسوفت جميع البرمجيات AV. ويمكنك أن تعرف إذا كــان برنامجــك AV مــدعوماً بالــذهاب إلى www.microsoft.com/security/partners/antivirus.asp. تضــم اللائحة الجزئية بالبرامج AV المدعومة Symantec، Trend Micro، Computer Associates، GFI، F-Secure، Sophos، Kaspersky، McAfee وPanda Software.

يضم المركز الأمني أيضاً الميزة Internet Options التي تسمح بإنشاء لائحة بمواقع الوب الموثوقة والمحجوزة، ضبط إعدادات الخصوصية على الوب، وتأهيل إعدادات الأمن الأخــرى. يغطي الفصل السابع هذه الخيارات.

ZoneAlarm من Zone labs

Zone labs هي شركة أمــن الكمبيــوتر (تملكهــا الآن، CheckPoint Software Technologies، مزود رئيسي للأعمال بمنتجات الأمن). وتصدر الشركة جدار نار مجــاني للإنترنت يدعى Zone Alarm، يمكن تحميله من موقع الوب www.zonelabs.com).

إن جدار النار ZoneAlarm المجاني هو برمجيات شاملة نظراً لأنه لا يكلفك شيئاً. يؤدي جدار النار ZoneAlarm خمس وظائف رئيسية: جدار النار، التحكم بالبرامج، مراقبة البرامج المضادة للفيروسات، حماية البريد الإلكتروني، والتنبيه والتسجيل.

جدار النار

يراقب جدار النار الوصلات الواردة لحمايتك من المتدخلين. يضم جدار النار منطقــتين أمنيتين تسمحان بضبط الإعدادات الأمنية. تتعامــل المنطقــة Internet Zone مــع جميــع الكمبيوترات على الإنترنت. أما المنطقة Trusted Zone فتحتوي على إعدادات للكمبيوترات التي تثق بها، مثل الكمبيوترات الموجودة على شبكة منــزلية وتتشارك الملفات معها.

التحكم بالبرامج

يراقب ZoneAlarm البرامج على كمبيوترك التي تطلــب وصــلات إلى الإنترنــت. وتساعدك آلية حماية الوصلات الصادرة على منع أحصنة طروادة، سباوير والــبرامج مــالوير الأخرى التي قد توجد على كمبيوترك من الوصول إلى الإنترنت. بعد تثبيت البرمجيات ينبهك ZoneAlarm في كل مرة يريد برنامجاً أن يصل إلى الإنترنت. أما بالنسبة للبرامج الموثوقة، مثل برامج استعراض الوب، برامج المحادثة أو البريد الإلكتروني، فسمح جدار النار تلقائياً بعمل هذه البرامج.

مراقبة البرامج المضادة للفيروسات

على الرغم من أن جدار النار المجاني لا يقوم بفحص الفيروسات ولكنه يراقب البرمجيات AV. وينبهك إذا كانت البرمجيات قديمة أو غير مؤهلة. على كل حال، ينجز هذه الوظــائف من أجل ثلاثة برامج AV فقــط: Norton AntiVirus مــن Norton، Viruscan مــن McAfee وEZ Antivirus من Computer Associates. لاحظ أن معظم الــبرامج AV تخبرك أيضاً عندما تكون قديمة.

حماية البريد الإلكتروني

تحجر هذه الميزة الملفات المرتبطة التي تصل عبر البريد الإلكتروني وهي الطريقة الرئيسية لانتشار الفيروسات والديدان. على كل حال، يحجر الإصــدار المجــاني مــن ZoneAlarm الارتباطات من النوع vbs. فقط. (VBS تعني نص برمجي فيجوال بيسيك وهي لغة كمبيوتر تم استخدامها بشكل شائع جداً بين مبرمجي الفيروسات ولكن نجمها أفل نوعاً مــا في هــذه الأيام).

التنبيه والتسجيل

تؤدي هذه الميزة وظيفتين: التنبيه هو رسالة منبثقة تحتاج إلى استجابة منك. وتتناول هذه الرسائل المنبثقة التنبيه إلى المعلومات (إعلام بأن شيء ما قد حــدث) والتنبيــه إلى البرنــامج (برنامج يحاول إنجاز وظيفة).

يمكنك أن تختار عرض كل التنبيهات أو عرض تنبيهات البرامج فقط. وقــد تريــد أن تعرض جميع التنبيهات في الأيام الأولى التي تستخدم فيها البرمجيات. فيعطيك ذلك فهماً أفضل لما يجري عندما تستخدم الإنترنت. على كل حال، قد تجد نفسك محاصراً بالرسائل المنبثقــة، وفي هذه الحالة يمكنك عرض تنبيهات البرامج فقط، فتتلقى تنبيهاً عند وجود نشاط مــؤذي جداً.

ويتم تسجيل نشاطات جدار النار، بما في ذلك حركة المرور التي يحجزها جدار النــار. يمكنك أن تعرض السجلات بنقر علامة التبويب Log Viewer في القسم Alerts & Logs. ويمكنك أن تنقر أيضاً إدخال سجل محدد لكي تحصل على مزيد من المعلومات عن الحدث.

5-3 جدران النار التي يمكنك شراؤها

لقد بحث القسم السابق في جداري نار مجانيين. كلاهما جيد جداً، ويمكنــك أن تجــد جدران نار أخرى بالبحث عن جدران النار الشخصية المجانية. "free personal firewall".

عندما تقارن جدار نار مجاني مع جدار نار بكلفة 50$، هل هناك أي مزايا تحصل عليها تقابل هذا الثمن؟ إذا كان الحديث عن جدران النار فقط، فإنني أجيب بنعم.

على كل حال، يوجد سبب وجيه لشراء جدار نار: تأتي العديد منها في حزمــة مــع منتجات أساسية من الإنترنت، مثل البرمجيات المضادة للفيروسات، الحماية من السبام وكشف السبايوير. وجدران النار لا توقف فيروسات البريد الإلكتروني أو السبام، لذلك فاجتماعها مع منتجات أخرى يجعلها تستحق الثمن الذي يدفع من أجلها. تقدم جدران النار التجارية أيضاً مزايا وخيارات تفوق الإصدارات المجانية، مثل خصوصية الوب، حجز النوافذ المنبثقة، والقدرة على تحديد وحجز الديدان المعروفة.

على سبيل المثال تضم المجموعة الأمنية ZoneAlarm جدار نار، برمجيات AV، ومزايا أخرى مثل الحماية من خداع البريد الإلكتروني والرسائل الفورية، حماية خصوصية الإنترنت، ومزايا أخرى غير موجودة في الإصدار المجاني.

توجد حزمة منتجات أخرى هي أمن الإنترنت نورتون من Symantec وتضم جدار نار، برمجيات AV، برمجيات مضادة للسبايوير، ومنتجات أساسية أخرى بما في ذلك الحماية من رسائل التصيد مع برمجيات مضادة للسبام وبرمجيات التحكم الأبوي لحماية ومراقبة الأطفال عند استعراضهم الوب.

تقدم حزمة أمن الإنترنت PC-cillin من Trend Micro أيضاً جدار نار شخصي، برمجيات AV، برمجيات مضادة للسبام، برمجيات مضادة للسبايوير، وحماية من هجوم التصيد.

وتقدم حزمة أمن الإنترنت من McAffee جدار نار شخصي، برمجيات AV، كشف وإزالة السبايوير، حماية من السبام، وبرمجيات خصوصية الوب في منتج واحد.

يسرد الجدول 3-1 منتجات جدران النار الشخصية الأكثر استخداماً في هذه الأيام. وتتراوح الأسعار من 39.95$ إلى 79.95$ (في منتصف 2005)، ولكن توجد عروض خاصة وإمكانية الحسم. يسرد الجدول 3-2 جدران النار المجانية.

الجدول (3-1):

جدران النار الشخصية الأساسية			
المنتج	البائع	موقع الوب	المزايا
Black ICE PC Protection	Internet Security Systems	www.blackICE.iss.net	جدار نار، كشف التدخل وأكثر من ذلك.
eTrust EZ Armor	Computer Associates	www.ca.com أو www.my-etrust.com	جدار نار، برمجيات AV، وأكثر من ذلك.
F-Secure Internet Security	F-Secure	www.f-secure.com	جدار نار، برمجيات AV، برمجيات مضادة للسبايوير وأكثر من ذلك.
Internet Security Suite	McAfee	www.mcafee.com	جدار نار، برمجيات AV، برمجيات مضادة للسبام، برمجيات مضادة للسبايوير وأكثر من ذلك.
Kaspersky Personal Security Suite	Kaspersky Lab	www.kaspersky.com	جدار نار، برمجيات AV، برمجيات مضادة للسبام،

جدران النار الشخصية الأساسية			
المنتج	البائع	موقع الوب	المزايا
			برمجيات مضادة للسبايوير وأكثر من ذلك.
Norton Internet Security	Symantec	www.symantec.com	جدار نار، برمجيات AV، برمجيات مضادة للسبام، برمجيات مضادة للسبايوير وأكثر من ذلك.
Panda Platinum Internet Security	Panda Software	www.pandasoftware.com	جدار نار، برمجيات AV، برمجيات مضادة للسبام، برمجيات مضادة للسبايوير وأكثر من ذلك.
PC-cillin Internet Security	Trend Micro	www.trendmicro.com	جدار نار، برمجيات AV، برمجيات مضادة للسبام، برمجيات مضادة للسبايوير وأكثر من ذلك.
Sygate Personal Firewall Pro	Sygate Technologies	www.sygate.com	جدار نار، كشف التدخل وأكثر من ذلك.
ZoneAlarm Security Suite	ZoneLabs	www.zonelabs.com	جدار نار، برمجيات AV، حماية البريد الإلكتروني وأكثر من ذلك.

الجدول (3-2):

جدران النار المجانية			
المنتج	البائع	موقع الوب	المزايا
Kerio Personal Firewall	Kerio Technologies	www.kerio.com	
Sygate Personal Firewall Standard	Sygate Technologies	http://smb.sygate.com/products/spf_standard.htm	
Windows XP Service Pack 2	Microsoft	www.microsoft.com/windowsxp/sp2/default.mspx	
ZoneAlarm	ZoneLabs	www.zonelabs.com	

كيف يجب أن تختار؟

إن المورد الأفضل الذي يساعدك على اختيار جدار النار المناسب هو الإنترنت والأشخاص الذين تعرفهم. ويوجد الكثير من المقالات، الآراء والمعلومات عن المنتجات الأمنية على الإنترنت. والطريقة الأفضل هي أن تدخل منتج معين في محرك بحث وتبدأ عملية البحث. وقد تحصل على عدد كبير من الارتباطات إلى الشركة التي تبيع هذا المنتج، وسوف تحصل على الأغلب على بعض الارتباطات غير المهمة.

ولكي تبحث بشكل هادف، انظر إلى الموارد على الوب مثل CNET.com. يحتوي هذا الموقع على مقالات عن العديد من منتجات أمن الكمبيوتر، بما في ذلك جدران النار الشخصية. وتسمح المنشورات مثل PC Magazine وPC World ببحث مواقع الوب الخاصة بها عن هذه المنتجات.

يوجد خيار ثان وهو أن تجرب بعضاً منها بنفسك. يمكن تحميل معظم جدران النار على الإنترنت، وهي تقدمٌ فترة تجريبية تتراوح بين 30 و90 يوم عادةً. كما يمكنك أن تستخدم التقييم الموجود في المجلات ونصائح زملائك لتخفض اللائحة إلى بندين أو ثلاثة ثم تختبر كلاً منها.

استفد من فترة الاختبار لكي تجد جدار النار الأفضل بالنسبة لك، أي منها يناسب ميزانيتك بشكل أفضل؟ أي منها يقدم واجهة المستخدم الأكثر جاذبية؟ أي منها تشعر بالارتياح بالعمل معه؟ أي منها يقدم الأفضل مع التنبيهات؟ أي الشركات يقدم أفضل دعم تقني؟ أي منها يجعلك تشعر بالأمن أكثر من غيره؟ لون أي منها هو الأفضل؟ مهما كانت معاييرك يمكنك أن تختبر المنتج الذي يناسبك تماماً. وبالفعل، إذا كنت تتحمل أزمان تحميل طويلة، يمكن أن تستغرق سنة لتغطية المنتجات المجانية بانتقالك من إصدار تجريبي إلى آخر.

6-3 اختبار جدران النار

كيف تعرف أن جدار النار يعمل؟ إحدى الطرق هي باختباره. تمسح العديد من مواقع الاختبار المتوفرة على الإنترنت كمبيوترك وتصدر تقريراً بالنتائج. نذكر فيما يلي بعض المواقع الجيدة التي تساعدك على رؤية منظر كمبيوترك من الخارج.

(www.grc.com) ShieldsUP!

يدير هذا الموقع الخبير ستيف جيبسون، وقد مسح الكثير من كمبيوترات المستخدمين لسنين (بالطبع مع سماحية المستخدمين). وهو طريقة رائعة لتبحث عن نقاط الضعف، مثل مشاركة ملفات ويندوز عن طريق NetBIOS والمنافذ العامة التي قد تكون مفتوحة (وهكذا يمكن للأشخاص السيئين الوصول من خلالها). النتائج واضحة وسهلة الفهم. ويضم الموقع

ارتباطات إلى معلومات كثيرة عن جدران النار الكمبيوترية وأمن الكمبيوتر.

يقدم هذا الموقع عدة اختبارات. اثنان منهما مفيدان على وجه الخصوص للمستخدمين المنـــزليين. يدعى الاختبار الأول المنافذ العامة ويدقق 26 منفذ مستخدم بشكل كـــبير (قـــد تكون مفتوحة ويمكن للأشخاص السيئين الوصول من خلالها). ويدعى الاختبار الثاني منافـــذ الخدمة ويدقق 1056 منفذ. وهو اختبار أشمل ويستغرق وقتاً أطول بقليل.

قد تؤدي مواقع اختبار أخرى وظائف مشابهة، ولكن لا يؤدي أي منها الاختبار بمستوى الحماس لدى موقع جيبسون. إذا كنت تختبر جدار نار لكي تعرف مقدار صموده في وجـــه المتدخلين على الإنترنت. يجب أن يكون هذا الموقع محطتك الأولى.

اختبار الأمن من Symantec

(www.symantec.com/homecomputing/)

يمسح اختبار الأمن من Symantec كمبيوترك بحثاً عن مختلف نقاط الضعف، بما في ذلـــك المنافذ التي قد تستجيب للطلبات غير المرغوبة، وجود برامج أحصنة طروادة، وفيما إذا كنت تشغل برمجيات مضادة للفيروسات. ونتائج الاختبار مفهومة (على الرغم من أنها أكثر جموداً من نتـــائج موقع جيبسون)، وتتوفر نتائج تفصيلية لاختبار القرصنة (الذي يبين المنافذ الـــتي تســـتجيب أو لا تستجيب لطلبات إقامة الوصلة). يحتاج الاختبار إلى تحميل أكتيف إكس لكي يعمل.

McAfee MySecurityStatus

(http://us.mcafee.com/MySecurityStatus/)

مثل اختبار الأمن من Symantec، يحتاج MySecurityStatus لتحميل أكتيف إكس لكي يدقق حالة جدار النار الشخصي والبرمجيات المضادة للفيروسات الموجودة لديك.

(www.pivx.com/preview) PivX Preview

أداة الأمن PreView مجانية ويمكن تحميلها من شركة تدعى PivX. تعطي هذه الأداة كمبيوترك مستوى أمني وفق أربع فئات: مركز تهديد، برمجيات أمن، رقع/تثبيت، وحماية جدار النار. وتحلل PreView كمبيوترك لتحسب العلامة الأمنية باستخدام هذه الفئات الأربعة. إنها طريقة بسيطة لوصف قابلية كمبيوترك لتلقي الهجوم. على كل حال، يعتمد جزء مهم مـــن العلامة على شرائك لمنتج آخر من PivX، لذلك فهذه العلامة غير دقيقة تماماً.

تؤدي الأداة عدداً من الوظائف (يتم شرحها بمزيد من التفصيل في الفصـــل الســـابع)، وأحدها إجراء اختبار أساسي لجدار النار. يمسح كمبيوترك عبر الإنترنت ليعرف المنافذ المفقودة ويختبر استجابتها للطلبات غير المرغوبة.

لكي تبدأ عملية المسح، انقر الرمز Firewall Protection. وقبل أن تبدأ عملية المسح، يجب أن تقبل بالاتفاقية التي يتم إجراء المسح وفقها. تنص الاتفاقية على أنك مالك الكمبيوتر وأنك مرخص لإجراء هذا الطلب. قد ينبهك كمبيوترك أن PreView ملف تنفيذي ويحاول أن يتصل بالإنترنت عندما تبدأ بالمسح. إنه أمر مقبول لذلك يمكنك أن تسمح بأداء هذه العملية.

تدقق عملية المسح 16 منفذاً عاماً، بما في ذلك المنفذ 80 (الوب) والمنفذ 25 (SMTP، بروتوكول لإرسال البريد الإلكتروني). يخبرك التقرير عن حالة كل من المنافذ (مفتوح أو مغلق) والهدف العام من كل منفذ. وإذا كان جدار النار لديك يعمل في النمط الصامت، يجب أن تحصل على علامة عالية. تذكر أن المنفذ المغلق أمثلي. ولا يعني ذلك أن برنامج استعراض الوب لن يتصل بالوب؛ بل يعني فقط أن جدار النار لن يستجيب للمحاولات غير المرغوبة بشأن فتح قناة اتصال.

(www.auditmypc.com) AuditMyPC

يدقق هذا الموقع المنافذ المتاحة في كمبيوترك. ويمسح أيضاً كمبيوترك من أجل سبايوير ونقاط الضعف في برنامج الاستعراض. ولكن النتائج غير واضحة بالجودة نفسها كما في المنتجات السابقة، لكن الموقع يسمح لك بمسح جميع المنافذ 65535 بدلاً من مسح المنافذ الأكثر استخداماً من المتدخلين. ويسمح أيضاً باختبار المنافذ المحددة.

7-3 لائحة التدقيق

استخدم هذه اللائحة كدليل مرجعي للمواد المغطاة في هذا الفصل.

ما يجب أن تفعله

- تثبيت برمجيات جدار النار على كمبيوترك واستخدام الإعداد "الصامت".
- تحميل ويندوز XP سرفيس باك 2 أو طلب قرص مضغوط من /www.microsoft.com windowsxp/sp2/default.mspx.
- استخدام جدار نار يشمل برمجيات مضادة للفيروسات، مضادة للسبايوير وإمكانيات أخرى.
- اختبار جدار النار باستخدام موقع أو أكثر من المواقع المذكورة في القسم "اختبار جدران النار".
- سؤال مصنّع جدار بشكل دوري عن التحديثات البرمجية.
- نسخ الملفات المهمة احتياطياً بشكل دوري.

ما يجب أن لا تفعله

- استخدام الإنترنت بدون جدار نار.
- الاعتقاد بأن جدار النار سوف يحميك من جميع مخاطر الإنترنت.

8-3 موارد مساعدة

يقدم هذا القسم موارد إضافية لمساعدتك على تعلم المزيد.

RTFM اختصار للجملة "اقرأ دليل التشغيل اللعين" فالعديد من الأسئلة تجد الأجوبة عليها في دليل تشغيل المنتج أو في مواقع الأسئلة المتكررة على الوب FAQ. وإذا وضعت سؤالاً بسيطاً على مواقع المساعدة على الوب، لا تُفاجأ إذا تلقيت هذا الجواب.

موقع الوب www.firewallguide.com هو مورد رائع عندما تتسوق منتجات عتاد وبرمجيات الأمن. يوجد لديه أطنان من المعلومات عن جدران النار والحلول الأخرى، بما في ذلك الأدوات المضادة للفيروسات والمضادة للسبايوير. ويجمع هذا الموقع المقالات من مجلات الكمبيوتر المشهورة، بما في ذلك مراجعات ومقارنات بين منتجات أمن المستخدم المنــزلي.

أسرار وكذب: الأمن الرقمي في عام الشبكات للكاتب بروس شناير. يقدم هذا الكتاب مقدمة رائعة عن أمن الكمبيوتر بما في ذلك جدران النار. ويتحدث أيضاً عن الضعف البشري في قلب كل نظام أمني (بما في ذلك الشكوى الدائمة لخبراء الأمن أن برمجيات الأمن الأفضل في العالم تقف عاجزة في مواجهة الأشخاص الذين ينقرون على الملفات المرتبطة). ويقدم مواضيع معقدة متسمة بالوضوح وروح الفكاهة.

الفصل الرابع

التخلص من الضيوف غير المرغوبين، الجزء 1: الفيروسات والديدان

نستخدم في هذا الكتاب المصطلح مالوير malware. وهو مصطلح عام يصف أي جزء من البرمجيات تم إنشاؤه لإيذاء نظام كمبيوتر. تشمل مالوير العديد من البرمجيات الخبيثة، بما في ذلك الفيروسات، الديدان، أحصنة طروادة وبعض السبايوير والأدوير عالية الخطورة.

يبحث هذا الفصل في أسباب هذا النمو الهائل لمالوير. ويناقش أيضاً نوعان محددان من مالوير: الفيروسات والديدان. سوف نشرح كيف تصل إلى كمبيوترك، والخطوات التي يمكنك اتخاذها لحماية نفسك. سوف ننظر أيضاً إلى نقاط قوة وضعف البرمجيات المضادة للفيروسات ونناقش طريقة حجز و/أو إزالة الفيروسات والديدان.

4-1 نمو المالوير

لقد ازدهرت مالوير لعدة أسباب. السبب الأول هو القدرة المتنامية للكمبيوترات في الاتصالات. ففي أواخر الثمانيات، كانت مالوير تنتقل عبر الأقراص المرنة؛ ولكي تلتقط فيروس، يجب أن تضع قرص مصاب في كمبيوترك. ومع نمو الإنترنت، انتقلت مالوير عبر مختلف وسائل الاتصال. تنتشر مالوير في هذه الأيام عبر البريد الإلكتروني والرسائل الفورية، مختلف بروتوكولات الإنترنت، وشبكة الوب العالمية.

السبب الثاني لازدهار مالوير هو التجانس المتزايد لبيئات الكمبيوتر. فمالوير المكتوبة لنظام تشغيل أو منصة عمل لا يمكنها أن تعمل على غيرها. وفي الأيام الماضية كان عدم التجانس عائقاً في وجه الإصابة، لأن الكمبيوترات كانت تعمل على أنظمة تشغيل مختلفة. أما في هذه الأيام فقد انحصر الاختلاف بنوعين: مايكروسوفت ويندوز وUNIX (بما في ذلك الخيارات الأخرى مثل لينوكس). وهناك التطبيقات العامة مثل مايكروسوفت أوفيس وبرامج الاستعراض التي تعمل على أنظمة تشغيل مختلفة. يستفيد المالوير من نقاط الخلل الأمنية في

أنظمة التشغيل والتطبيقات ويستغلها كوسائل لإصابة نظام الكمبيوتر. عندما تجمع بين بيئة كمبيوترية متجانسة ومختلف عناصر الإصابة التي تعتمد على الشبكة، تكون النتيجة إصابة سريعة وواسعة للكمبيوترات المنـزلية وكمبيوترات الشركة والإنترنت على حدّ سواء.

أما السبب الثالث لازدهار مالوير فهو أن أدوات الدفاع التقليدية ضد مالوير تعتمد على رد الفعل. إن البرمجيات المضادة للفيروسات والمضادة للسبايوير فعالة جداً ضد أنواع الهجوم المعروفة. ولكن عندما يظهر نوع جديد من مالوير، تتوفر الفرصة لكي ينتشر مالوير ريثما تحلل مجموعات البحوث الأمنية الهجوم، تحضر برنامجاً مضاداً وتوزعه. إن الأشخاص المسيئون يملكون المبادرة، ويستخدمونها لمصلحتهم. ويمكن أن تمنع جدران النار الوصول إلى قنوات الاتصال غير العادية، لكن يوجد قسم كبير من مستخدمي الإنترنت لا يملكون جدار نار أو أنهم يستخدمونه بإعداد غير مناسب. ويستخدم المهاجمون أيضاً القنوات العامة مثل الويب أو البريد الإلكتروني لنشر مالوير. ويتم تطوير بعض التقنيات التي يمكنها كشف وحجز أنواع جديدة وغير معروفة من الهجوم، لكن العمل ما يزال جارياً على هذه التقنية؛ وهي تسبب مشاكل غالباً مع البرامج والتطبيقات الشرعية.

والسبب الرابع والأهم لازدهار مالوير هو المال. فمؤسسات الأعمال سيئة السمعة والمنظمات الإجرائية تربح نقوداً من كتابة البرامج التي لا تريدها على كمبيوترك. كان الاعتقاد السائد سابقاً بأن حافز مبرمجي مالوير هو السلوك المعادي للمجتمع؛ وأنهم يكتبون برامج مالوير ليفاخروا بعملهم ولكي يرضوا غرورهم. لكن مالوير سريعة الانتشار تجلب الشهرة في مجتمع الكمبيوتر كما تفعل الأغنية الناجحة الجديدة لمغني أو رواية تحقق أفضل المبيعات لكاتبها. (إذا كنت ترغب بمعرفة المزيد حول هذا الموضوع، انظر إلى بحث سارة غوردون في الموقع www.badguys.org/papers.htm).

لكن إدخال المال في المعادلة يغير الصورة. فبمبرمجي مالوير الذين يعملون من أجل المال لا يرغبون بإحداث ضجة كبيرة، بل ينشئون برامج صامتة تعمل بهدوء وتخترق الكمبيوترات وتبقى فيها أطول فترة ممكنة. أما مالوير التي يتم الحديث عنها في الصحافة يتم التقاطها وإزالتها أيضاً. إن مالوير التي تجلب الأرباح تحاول أن تعمل في الخفاء.

توجد ثلاثة طرق لجلب المال من كتابة البرمجيات الخبيثة القادرة على الانتشار. الطريقة الأولى هي التجسس، فالشركات والحكومات هي أهداف دائمة للجواسيس الذين يحصلون على المال من سرقة أسرار الحكومة أو الملكية الفكرية. (على سبيل المثال، تم إصدار تقرير في أيار 2005 أنه تم توقيف ثلاثة مدراء شركات لتوظيفهم رجال تحري من

أجل التجسس على منافسيهم. وقد استخدم رجال التحري برمجيات أحصنة طروادة لسرقة الملفات والمستندات من الكمبيوترات المصابة. وفي حالة سابقة، استخدم القراصنة الدودة QAZ لكي يصلوا إلى بعض شيفرة المصدر لمايكروسوفت في 2000). إن البرامج الخبيثة مثل مسجلات ضربات المفاتيح والأطقم الجذرية هي جزء من أدوات التجسس الرقمي. (الأطقم الجذرية Rootkits هي برامج تستقر في نظام تشغيل الكمبيوتر وتمنح المهام تحكماً كاملاً بالكمبيوتر. ويستطيع المهاجم أن يعود إلى الكمبيوتر المسيطر عليه بهذه الأطقم عندما يرغب بذلك ويشغل العمليات التي يختارها. كما تستطيع الأطقم الجذرية المبرمجة بإتقان أن تخفي نفسها عن مدراء الكمبيوتر. وتحتاج إلى أدوات متخصصة لكشفها وإزالتها). ومع أن التجسس الرقمي كان موجوداً منذ نشوء الكمبيوترات، فإن الأطقم الجذرية ليست مجرد أدوات للعمليات المختارة؛ بل توجد أطقم جذرية مبيتة بشكل مسبق على الإنترنت لأي شخص مهتم بالحصول على أحدها.

الطريقة الثانية لجلب المال من كتابة مالوير هي بالوصول إلى عدد كبير من الكمبيوترات ثم تأجيرها إلى مرسلي السبام والمحتالين. يمكن أن تكتشف مالوير المؤتمتة وتخترق وتتحكم بآلاف الكمبيوترات وتجندها كأجهزة تابعة يمكن التحكم بها عن بعد. تدعى أحياناً هذه الأجهزة التابعة زومبي أو البيرقانة، ويتم تأجيرها لإرسال السبام أو لبدء هجوم رفض الخدمة (DOS). (يغمر الهجوم DOS الموقع المستهدف بحركة مرور هائلة فيعجز المستخدمون المقبولون عن الوصول إليه). إن الكمبيوترات المنزلية مع وصلات DSL أو مودمات الكابل هي أهداف شائعة لأنها غالباً ما تكون غير محمية، وعرض المجال الكبير لوصلة الإنترنت التي تستخدمها يسمح بإرسال آلاف الرسائل الإلكترونية أو إقامة آلاف الوصلات إلى موقع الوب في الثانية الواحدة. يستطيع مرسلو السبام (ومؤخراً مرسلو رسائل التصيد) استئجار هذه الشبكات زومبي من أجل ابتزاز النقود من مواقع المقامرة والتعري على الوب بتهديدها بالهجوم "DOS" وتعريضها للإفلاس. ويفترض خبراء الأمن أن المجرمين قد يبدؤون باستهداف الأعمال النظامية أيضاً.

والطريقة الثالثة لتحقيق الأرباح من مالوير هي بالسرقة التي يتم التمهيد لها بسبايوير أو باستخدام الإعلانات التي تولدها أدوير عالية الخطورة. يمكن أن تسجل سبايوير، مثل مسجلات ضربات المفاتيح، معلومات حساسة كالمعرّف ID لحسابك المصرفي وكلمة المرور وترسلها إلى المهاجم الذي يستخدمها لتحريك النقود من حسابك. وتسهّل برامج أدوير عرض الإعلانات على كمبيوترك. وفي بعض الحالات، تجمّع هذه البرامج المعلومات من كمبيوترك، بما في ذلك المعلومات المتعلقة ببرنامج استعراض الإنترنت أو النشاطات الأخرى، وترسل هذه المعلومات إلى كمبيوتر بعيد أو موقع آخر على الإنترنت. تدفع الشركات لمبرمجي أدوير لقاء الإعلانات المنبثقة عندما تزور موقع منافس أو تزور مواقع متعلقة بالمنتجات والخدمات

المعروضة. وتصدر أدوير أيضاً تقارير عن نشاطك على الإنترنت وترسلها إلى الشركة الأم التي تجمّع المعلومات وتبيعها "كبحث المستهلك". وفي حين أن أحصنة طروادة والفيروسات هـي برامج خبيثة (وفي بعض الأحيان غير قانونية)، تشغل أدوير المنطقة الرمادية. ومعظم بـرامج الأدوير الموجودة على الإنترنت تم إنشاؤها في شركات (وليس في مؤسسات إجرامية أو مـن قبل مبرمجين مستقلين). ويوجد لدى هذه الشركات لائحة زبائن يستخدمون خدماتها من أجل الإعلانات أو إجراء بحث السوق ويحافظون على اسمهم وسمعتهم، مثـل جميـع الشـركات الأخرى. (يتم نقاش أدوير بمزيد من التفصيل في الفصل الخامس، التخلص م الضيوف غـير المرغوبين" الجزء 2: سبايوير، أدوير وأحصنة طروادة").

إن الهدف من هذا النقاش هو توضيح أن مالوير هي مشكلة جدية سوف تستمر بإصابة كمبيوترات المستخدمين حتى آخر الوقت. وبمعرفة التهديدات الموجودة في بيئة عملك، يمكنك اتخاذ الخطوات الضرورية لحماية نفسك.

ليست الغاية أن تجعل كمبيوترك منيعاً، فهذا أمر مستحيل. لكـن الإنترنـت مليئـة بالأهداف السهلة، وهدفنا هو أن تصبح هدفاً صعباً.

2-4 الفيروسات والديدان

الفيروس هو برنامج أو شيفرة تنسخ نفسها في الملفات الأخرى التي تتصل معها. ويصيب الفيروس برنامجاً آخراً، قطاع الاستنهاض، قطاع الأجزاء أو مستند يدعم برامج الماكرو وذلك بإدخال أو بربط نفسه مع هذا الوسط. ومعظم الفيروسات تنسخ نفسها فقط، لكن العديـد منها يدمر نظام الكمبيوتر أو بيانات المستخدم أيضاً (يدعو الباحثون ذلك حمولة الفـيروس). وفي بعض الأحيان يحتاج الفيروس إلى تشغيله لكي ينسخ نفسه، مثل نقر برنامج يحتوي علـى الفيروس أو فتح ملف مصاب. وبعد تنشيطه، ينسخ الفيروس نفسه ويصيب البرامج الأخرى أو ينتشر عبر آليات الاتصالات مثل البريد الإلكتروني. يقدم الجدول 4-1 معلومات إضافية عـن الأنواع المختلفة من الفيروسات.

تسهل الديدان توزيع النسخ وبدون أي تدخل بشري غالباً. ويمكن أن تخرب الديـدان الكمبيوترات وتخترق أمنها. فقد تصل إلى الكمبيوتر باستغلال نقطة خلل في النظام، أو عندما يفتح مستخدم رسالة بريد إلكتروني مصابة أو ينقر على ملف مرتبط بالرسالة. وعلى العكس من الفيروسات فإن الديدان لا تصيب ملفات المضيف. وبدلاً من ذلك، يتم بناؤها كـبرامج مكتفية ذاتياً تعمل بشكل مستقل عن البرامج الأخرى الموجودة في الكمبيوتر. وبالإضـافة إلى استخدام وسائل الاتصال مثل البريد الإلكتروني أو الرسائل الفورية، تملك بعض الديدان محرك مبيت يسمح بانتشارها عبر الإنترنت وعبر الشبكات المحلية. يقدم الجـدول 4-2 معلومـات إضافية عن الديدان.

الجدول (4-1):

مصطلحات الفيروسات		
النوع	**أمثلة**	**الوصف**
فيروس ملفات	Cascade	تربط فيروسات الملفات نفسها إلى البرامج، الملفات التنفيذية، والنصوص البرمجية. وإذا تم تشغيل ملف مصاب على كمبيوتر، يمكن أن ينتشر الفيروس إلى البرامج الأخرى.
فيروس ماكرو	Concept ،Melissa	الماكرو هو برنامج صغير يوجد ضمن تطبيق أكبر مثل مايكروسوفت وورد. ويهدف إلى تبسيط إدارة المهام العامة. يمكن أن تنسخ فيروسات الماكرو نفسها، تحذف أو تغير المستندات وتؤدي وظائف خبيثة أخرى.
فيروس قطاع الاستنهاض	Michelangelo	يخبر قطاع الاستنهاض في القرص أو القرص الصلب الكمبيوتر عن البرامج التي يجب تشغيلها عند قراءة القرص أو طريقة إقلاع نظام التشغيل. ويتم تنفيذ فيروسات قطاع الاستنهاض في كل مرة يتم استخدام القرص أو يتم تشغيل الكمبيوتر.
الفيروسات المقيمة في الذاكرة	Jerusalem	فيروس يقيم في ذاكرة الكمبيوتر بعد تأهيل شيفرة الفيروس.
الفيروس المتعدد	Zmist ،Marburg	فيروس يمكن أن يغير نموذج البايت الذي يستخدم عندما ينسخ نفسه، وبذلك يتجنب أن يتم كشفه بتقنيات مسح السلاسل البسيطة.
فيروس ريترو Retro	Gobi	فيروس يهاجم بقوة البرامج المضادة للفيروسات أو برامج منع الكشف.

يتم تصميم الديدان في هذه الأيام لتستفيد من نقاط الخلل الموجودة في أنظمة التشغيل أو التطبيقات الشائعة. تسمح نقاط الخلل بوصول الديدان إلى الكمبيوتر، وأداء أي مهمة موكلة إليها، ثم تنسخ نفسها لكي تصل إلى كمبيوترات أخرى تعاني من خلل في نظـام التشـغيل. أحياناً يكون بائعو البرمجيات على دراية بنقاط الخلل، ويصدرون تحديث للبرمجيات تدعى رقع أمنية. وفي أحيان أخرى، لا يعرف بائع البرمجيات أنه توجد مشكلة حتى تظهر دودة أو برنامج

مالوير جديد ويشق طريقه عبر الإنترنت، فيصدر البائع تحديثاً بسرعة. وفي كلتا الحالتين، يتعلق الأمر بالمستخدم من أجل البحث عن الرقع وتطبيقها. ومن أسباب نجاح الديدان أن العديد من المستخدمين لا يعرفون كثيراً عن تثبيت الرقع على كمبيوترالهم. يبحث الفصل السابع "تأمين ويندوز" الرقع الأمنية بمزيد من التفصيل.

الجدول (4-2):

مصطلحات الديدان		
النوع	**أمثلة**	**الوصف**
دودة	Bugbear، Netsky، Mydoom	الدودة هي برنامج يعمل على توزيع نسخ عنه، مثلاً من محرك قرص إلى آخر أو بنسخ نفسه باستخدام البريد الإلكتروني أو آلية نقل أخرى وقد تؤذي الدودة وتخترق أمن الكمبيوتر كما يمكن أن تصل إلى الكمبيوتر باستغلال خلل في النظام أو عندما تنقر على بريد إلكتروني مصاب.
الدودة Mailer و-mass-mailing	LoveLetter (مرسل البريد بأعداد كبيرة)، Happygg (مرسل البريد)	الديدان المرسلة للبريد بأعداد كبيرة والمرسلة للبريد هي فئة خاصة من ديدان الكمبيوتر ترسل نفسها في البريد الإلكتروني. يرسل النوع الأول عدة نسخ منه، بينما يرسل النوع الثاني نفسه بمعدل أقل.
التهديدات المختلطة	Nimda، Slammer، Blaster	تستفيد التهديدات المختلطة من مميزات الفيروسات، الديدان، وأحصنة طروادة وخلل البرمجيات لكي يبدأ، يرسل وينشر الهجوم. تشمل مميزات التهديدات المختلطة قدرتها على الأذية، الانتشار بطرق متعددة، والهجوم من عدة نقاط، فتنتشر بدون تدخل بشري وتستغل خلل البرمجيات. بفضل استخدام عدة طرق وتقنيات، يمكن أن تنتشر التهديدات المختلطة بسرعة وتسبب أذية كبيرة.

كما ذكرنا، لا تعتمد الديدان على التدخل البشري. فإذا كانت الدودة قادرة على إقامة وصلة إلى كمبيوترك، ويوجد خلل مناسب في البرمجيات الموجودة على كمبيوترك، ولم تستخدم أي حماية، فإن اللعبة تكون قد انتهت.

ما الذي يمكن أن تفعله الديدان والفيروسات؟

يتم إنشاء الديدان والفيروسات لكي توصل برمجيات إلى الكمبيوتر المستهدف. ويتم تصميم البرمجيات لإنجاز وظيفة محددة، مثل حذف أو تغيير البيانات، تثبيت البرمجيات على كمبيوترك أو إنشاء باب خلفي يمكن أن يستهدفه المهاجم لاحقاً في الوصول غير المرخص إلى كمبيوترك.

تسبب الديدان والفيروسات المشاكل في الكمبيوترات المصابة، لكن تسبب أذية جانبية أكبر بسبب حركة المرور على الشبكة التي تولدها عندما تنتشر عبر الإنترنت. على سبيل المثال، SQL Slammor، دودة سريعة الحركة أصابت الملقمات التي تشغل إصدار مايكروسوفت SQL سيرفر 2000 الذي يحتوي على خلل. (SQL تعني لغة الاستعلام البنيوية، المستخدمة في قواعد البيانات). بعد إطلاق الدودة SQL Slammer في كانون الثاني 2003، سيطرت هذه الدودة بسرعة على الكمبيوترات التي تحتوي على خلل وبدأت بالبحث عن ضحايا جدد، وعندما بلغت ذروة انتشارها، تضاعف عدد الكمبيوترات التي تم السيطرة عليها كل 8.5 ثانية. وأدى الفيضان المروري الناتج عن الوصول إلى الكمبيوترات إلى تجميد الإنترنت. وفقدت معظم كوريا الجنوبية الوصول إلى الإنترنت، كما اضطرت شركة الخطوط الجوية Continental Airlines لإلغاء الرحلات من المجمع المركزي Newark، وخرجت العديد من كوى ATM المصرفية عن الخدمة لساعات.

لقد تم استخدام الديدان والفيروسات لكي توجد في فئات منفردة، ولكنها في السنين القليلة الماضية بدأت بالتعاضد لإنشاء تهديدات متعددة وبطرق متعددة لكي تنشر نفسها. على سبيل المثال، تنتشر العديد من الديدان (تدعى مرسلات البريد بأعداد كبيرة) عبر البريد الإلكتروني. وتستخدم ديدان أخرى مختلف آليات الانتشار.

الدودة Nimda هي مثال جيد، ظهرت في 18 أيلول 2001، واستخدمت خمس طرق مختلفة للانتشار. الطريقة الأولى بإجراء مسح للملقمات ويندوز التي تشغل إصدار مع خلل في IIS (IIS هو ملقم معلومات إنترنت وهي برمجيات ملقم الوب لمايكروسوفت). وبمجرد اختيار ملقم، فإنها تستخدمه كمحطة للبحث عن كمبيوترات أخرى تحتوي على هذا الخلل. ويمكنها أن تنتشر أيضاً عبر أوتلوك (برمجيات البريد الإلكتروني لمايكروسوفت) إلى العناوين الموجودة في دليل عناوين الضحية. وثبتت الدودة Nimda نفسها أيضاً على كمبيوترات الأشخاص الذين تحولوا إلى ملقم وب مصاب بالدودة Nimda، حمّلت شيفرتها عبر إنترنت

إكسبلورر (برنامج استعراض مايكروسوفت). وانتشرت أيضاً عبر مشاركة الملفات في ويندوز (آلية مايكروسوفت لمشاركة الملفات بين الكمبيوترات) وعبر الأبواب الخلفية الموجودة مسبقاً والتي تم تثبيتها بدودتين سابقتين هاجمتا ملقمات IIS ويندوز.

3-4 البرمجيات المضادة للفيروسات

يمكنك أن تحمي كمبيوترك من الإصابة بالفيروسات والديدان بطرق مختلفة. والحماية الأفضل من الفيروسات والديدان هي باستخدام البرمجيات المضادة للفيروسات (AV). ويمكن أن توقف البرمجيات AV تثبيت الفيروسات وتكشف، تحجر، وتزيل الفيروسات والديدان من كمبيوترك والتي انسلت خلف خطوط دفاعك.

تعمل البرمجيات AV التقليدية بأخذ توقيع عن كل فيروس أو مالوير. يحدد التوقيع قسم من الشيفرة التي تظهر في البرنامج مالوير فقط. وبالتالي فإن التوقيع يشبه البصمة؛ ويقدم دليل قوي على هوية البرنامج. في كل مرة تمسح البرمجيات AV ملف مرتبط مع البريد الإلكتروني أو تختبر الملفات على قرصك الصلب، فإنها تبحث عن بصمات الفيروسات والديدان المعروفة.

ما الذي يمكن أن تفعله البرمجيات AV

يمكن أن تحميك البرمجيات AV من الفيروسات المعروفة التي تظهر في أماكن متعددة: البريد الإلكتروني الوارد والصادر، الرسائل الفورية، ومحرك القرص الصلب في كمبيوترك. يجب أن تعدّ البرمجيات AV لكي تمسح الرسائل الواردة والصادرة بشكل تلقائي. وإذا استخدمت بريد الوب من مزودات الخدمة مثل MSN، AOL وYahoo!، فإن مزود الخدمة يمسح بريدك الإلكتروني أيضاً من الفيروسات. (يستخدم MSN منتجات مسح الفيروسات من Trend Micro، ويستخدم Yahoo! البرنامج Norton Anti Virus، ويستخدم AOL البرنامج McAFee).

تأتي معظم المنتجات المضادة للفيروسات مع ماسح بالزمن الحقيقي يدقق ملفاتك في كل مرة تصل إليها. يجب أن تمسح أيضاً محرك القرص الصلب بشكل دوري لتبحث عن برامج المالوير التي قد وجدت طريقها إلى كمبيوترك. تشغّل معظم البرمجيات AV عمليات مسح مجدولة بفترات دورية، ولكن يمكن أن تستغرق عمليات المسح وقتاً طويلاً (يستغرق المسح الكامل لكمبيوتري المحمول أكثر من 90 دقيقة) ويمكن أن تبطئ التطبيقات الأخرى. يمكنك أن تقاطع المسح المجدول إذا وجدت أنه يتعارض مع عملك، ولكن يجب أن تشغل المسح الكامل كلما أمكن ذلك. ينصح بعض الخبراء بإجراء المسح مرة في الأسبوع، لكنني أعتقد أن الأشخاص الموسوسين فقط يفعلون ذلك. إذا كان بإمكانك إجراء المسح مرة في الشهر، فأنت في حال جيدة.

ما الذي لا يمكن أن تفعله البرمجيات AV

لا يمكن أن تحميك آليات الحماية في البرمجيات AV التقليدية من الفيروسات التي لا يعرف بائعو AV عنها شيئاً. وكما قد تكون عرفت من الفقرة التي تتحدث عن التواقيع، فإن سيئة الكشف المعتمد على التواقيع هي أن الشركة AV بحاجة للحصول على نسخة من الفيروس لإنشاء التوقيع. وعندما تواجه فيروسات جديدة لم يراها أحد قبلاً، فلن تساعدك البرمجيات AV. تحصل البرامج مالوير الجديدة على حرية الحركة حتى تحلل الشركات AV البرنامج مالوير، تنشئ توقيع، وتوزعه إلى زبائنها. تحدث هذه العملية عادةً خلال 3 أو 4 ساعات من ظهور الفيروس، أما إذا كنت غير محظوظاً ووقعت بين الموجة الأولى من الضحايا، فيجب أن تنتظر حتى يصدر البائع أداة إزالة لبرنامج مالوير. لمزيد من المعلومات، انظر إلى الشريط الجانبي في نهاية الفصل، "إزالة إصدار الدودة Beagle").

توجد تقنيات تحاول أن توقف برامج مالوير غير المألوفة باختبار سلوك البرمجيات والبحث عن المؤشرات التي ستقوم بشيء مؤذ أو غير مرغوب على الكمبيوتر. على سبيل المثال، تضم العديد من المنتجات AV محرك مساعد يبحث عن مميزات الفيروس ضمن الشيفرة. وهذه الشيفرة نفسها غير فعالة في كشف حصان طروادة أو الدودة في نظام التشغيل ويندوز. لقد أثبتت المحركات المساعدة نفسها بأنها ذات فعالية كبيرة في كشف الأشكال المختلفة من برامج مالوير المعروفة أو الفيروسات المتعددة. يتم تنفيذ الأشكال المختلفة لبرنامج مالوير معروف بإجراء تغيير عليه لمحاولة تجنب كشف التوقيع، تغير الحمل البرمجي للهجوم أو تعديل الآلية التي يستخدمها مالوير. تضم الديدان في هذه الأيام مئات أو آلاف الأشكال التي يتم إصدارها حول الهجوم الأصلي. الفيروسات المتعددة هي فيروسات تم برمجتها لتغير شيفرتها بفترات دورية لكي تتجنب عمليات المسح المعتمدة على التوقيع وتحاول الاستمرار في تأدية الوظيفة نفسها.

على كل حال، مع أن الكشف المساعد يمكن أن يكون فعالاً جداً ضد فئات من التهديدات المعروفة، فإنه لا يغطي جميع أنواع التهديدات. توجد تقنية تدعى حلول منع التدخل في المضيف (HIPS)، يمكنها أن توقف عمليات الهجوم غير المعروفة باختبار الشيفرة والبحث عن مؤشرات السلوك الخبيث. تمنع هذه التقنية أيضاً هجوم طفح الدارئ وهو هجوم شهير لبرامج المالوير. يرسل طفح بيانات إلى منطقة من ذاكرة الكمبيوتر (تدعى دارئ) أكثر مما يتوقعه الكمبيوتر. وتملأ البيانات الإضافية دارئ الذاكرة ويتم تشغيلها في الكمبيوتر، وأثناء استغلال طفح الدارئ فإن هذه البيانات الإضافية تكون عادة شيفرة الهجوم، مما يعطي المهاجم القدرة على التحكم بالكمبيوتر. تستخدم الديدان عادة طفح الدارئ، بما في ذلك Code Red، Nimda وSasser.

إن التقنية HIPS هي تطوير مهم في الأمن لأنها تقنية وقائية؛ أي أن الكمبيوترات محمية من عمليات الهجوم غير المعروفة بدون الحاجة إلى الانتظار ريثما يتم تسليم التواقيع الجديـــدة. تتزايد الحاجة إلى استخدام التقنية الوقائية بسبب عمليات الهجوم الجديدة التي تنشئ بشـــكل متكرر وتنتشر بسرعة فيمكنها إيقاع آلاف أو مئات الآلاف من الضحايا قبل أن يتم الحصول على التواقيع الضرورية لعمل البرمجيات المضادة للفيروسات.

لكن السيئة الرئيسية للتقنية HIPS هي أنها تخطئ غالباً وتحاول أن تمنع البرامج النظامية من العمل. عندما يحدث ذلك يدعى كشف خاطئ. وقد ابتلت عمليات الكشـــف الخـــاطئ تقنيات الكشف لسنوات وكانت السبب الرئيسي لاستمرار العمل في التقنية المعتمـــدة علـــى التواقيع - فمع أنها تعتمد على رد الفعل، لكنها دقيقة.

بالإضافة إلى ذلك، فإن معظم التقنيات HIPS توجهت إلى بيئات الشركات، حيـــث يمكن لمدير الشبكة أن يعرّف بشكل أفضل سياسات الأمن التي تحدد طريقة عمـــل حلـــول HIPS. ومع مضي الوقت وفهم هذه التقنيات بشكل أفضل، سوف تظهر منتجات جديـــدة موجهة للمستخدمين. وتتوافر عدد من المنتجات الأمنية، بما في ذلك التقنيات HIPS مثل حماية طفح الدارئ وأحد الأمثلة عنها TruPrevent Personal من الشـــركة Panda Software. وقد تم تصميمه كملحق للمنتجات AV لأن الهدف منه هو كشف عمليات الهجوم الـــتي لا يوجد تواقيع عنها. إذا كنت مهتماً بهذه التقنية، تسمح لـــك الشـــركة Panda Software بتجريب TruPrevent قبل أن تشتريه. أنصح بأن تستفيد من الفترة التجريبية لكي تعرف فيما إذا كانت هذه البرمجيات تتداخل مع وظائف الكمبيوتر العادية.

4-4 طرق الحماية الأخرى

لا تحميك البرمجيات AV دوماً من الديدان التي تستخدم وسائل اتصال غـــير البريـــد الإلكتروني أو الرسائل الفورية. قد تعثر البرمجيات AV على الديدان (أو برامج مالوير الأخرى التي تنقلها الديدان إلى الكمبيوترات المستهدفة) أثناء مسح القرص الصلب. ولكن لكي تمنعها من إصابة كمبيوترك يجب أن تتبع الخطوات المشروحة في بقية هذا الفصل.

استخدام جدار نار

كما تم شرحه في الفصل الثالث، "جدران النار"، يمكن أن يحجب جدار النار كمبيوترك عن الكمبيوترات الأخرى على الإنترنت. عندما تعدّ جدار النار بشكل مناسب، فإن الديدان التي تمسح الإنترنت بحثاً عن الكمبيوترات التي تحتوي على نقاط خلل، تتجاوز كمبيـــوترك. لنفترض استخدام حزمة برمجيات أمنية تقدم مزايا متعددة في منتج واحد، بما في ذلك البرمجيات AV، جدار نار، برمجيات مضادة للسبايوير وهكذا. تتضمن بعض جدران النار والبرمجيـــات

AV أيضاً كشف التدخل والتقنية الوقائية، والتي تبحث في حركة المرور الواردة من الإنترنت عن تواقيع الديدان المعروفة أو برامج مالوير الأخرى. على سبيل المثال، تتضمن البرمجيات Norton Anti Virus وظائف كشف التدخل الأساسية، في حين أن البرمجيات Norton Internet Security تتضمن جدار نار كامل مع كشف التدخل والوقاية. يمكن أن تحجز برمجيات كشف التدخل والوقاية أي برنامج مالوير تملك توقيعه وتقدم الحماية لبعض نقاط الخلل الجديدة في نظام التشغيل والتي لم يستغلها برنامج مالوير بعد. كما تضيف وظائف كشف التدخل والوقاية طبقة أخرى من الحماية من المخاطر الأمنية.

لا تفتح رسالة البريد الإلكتروني الغريبة

إن البريد الإلكتروني هو أفضل وسيلة تستخدمها الفيروسات منذ نشوء الكمبيوتر. يقدم البريد الإلكتروني آلية اتصال لانتشار الفيروسات، ويملك لائحة بالمضيفات الجديدة لإصابتها (جميع العناوين الموجودة في دليل العناوين)، ويسمح لمنشئ الفيروس بممارسة بعض الهندسة الاجتماعية ليحث الناس على فتح الرسالة، وبالتالي تسهيل انتشار الفيروس. لذلك يجب أن تحذر عند مراجعة الرسائل الموجودة في صندوق بريدك. فإذا رأيت رسالة من شخص لا تعرفه، دقق الأمور التالية:

- هل يحتوي عنوان المرسل :From على اسم غريب أو هل اسم الميدان غريب؟ (الميدان هو المعلومات الموجودة على يمين الإشارة @).
- هل سطر الموضوع :Subject يحتوي على أحرف عشوائية بدلاً من النص؟ (يشير ذلك إلى كتابة الرسالة بلغة لا يدعمها مستضاف البريد الإلكتروني، لذلك لا يمكنه تشكيل النص الأجنبي بشكل مناسب). وجود سطر موضوع فارغ يعطي إشارة تحذير أخرى.
- هل يحتوي سطر الموضوع :Subject على معلومات عن البيع أو إشارة تحذيرية من الحساب؟ (يستخدم العديد من مرسلو السبام ورسائل التصيد مبرمجي الفيروسات لإضافة مالوير إلى بريدهم التافه. يمكن أن تنجز مالوير كل أنواع الوظائف، من تسجيل ضربات المفاتيح إلى تحويل كمبيوترك إلى مرسل سبام قوي).
- هل تلقيت عدة رسائل بريد إلكتروني من المرسل نفسه أو رسائل بريد إلكتروني مع أسطر موضوع متشابهة بشكل مثير للشبهة؟

إذا أجبت على أي من هذه الأسئلة بنعم، يجب أن تحذف الرسالة قبل أن تفتحها. وذلك لأنه يتم تفعيل بعض برامج مالوير عندما تفتح الرسالة. إذا لم ترغب بحذفها، لا تفتحها وانتظر يوماً أو بضعة أيام. واذهب إلى موقع الوب لبائع البرمجيات AV لكي تبحث عن أخبار الفيروسات والديدان الجديدة. تضم التحذيرات الجديدة غالباً معلومات لمساعدتك على تحديد الفيروسات في صندوق بريدك، كسطور المواضيع المستخدمة في الفيروسات.

لا تنقر على أي ارتباطات أو برامج في رسائل البريد الإلكتروني

إذا فتحت رسالة غريبة، لا تنقر أي ارتباطات أو برامج متضمنة في الرسالة. حتى لــو كنت تعرف الشخص المرسل، فربما هذا المرسل قد وقع ضحية للفيروس. إن فيروسات وديدان إرسال البريد بأعداد كبيرة تستخدم دليل عناوين الضحية لكي ترسل نفسها إلى أكبر عدد من الضحايا، فتستغل بذلك الثقة بين المتراسلين. إذا اشتبهت بارتباط أرســله شــخص تعرفــه، استخدم طريقة أخرى كالاتصال الهاتفي لكي تضمن أن المرسل قد أرسل فعلاً الرسالة وأنــه يمكن استخدام الارتباط أو البرنامج بشكل مناسب. يوجد خيار آخر بإعادة كتابة الارتبــاط مباشرة في برنامج الاستعراض بدلاً من النقر عليه. وبهذه الطريقة تعرف أنك لن تنتقل إلى موقع خبيث إذا كان الارتباط يحتوي على حروف مخفية.

حافظ على تحديث جميع البرمجيات

تظهر فيروسات وديدان جديدة بشكل دائم، لذلك يجب أن تحــدّث البرمجيــات AV باستمرار. وإذا كانت البرمجيات AV التي تستخدمها تدعم عملية التحديث التلقائي، يجب أن تختار ذلك، لأنه يتم تسليم تواقيع جديدة بالإضافة إلى عمليات تحديث أخرى إلى كمبيوترك بدون أن تتكلف عناء ذلــك. علــى ســبيل المثــال، يمكنــك أن تؤهــل في البرمجيــات Norton AntiVirus الميزة Automatic Live Update وهــي خدمــة ترســل تعــاريف الفيروسات الأحدث وعمليات التحديث على البرامج إلى كمبيوترك عندما تتصل بالإنترنت.

يمكنك أن تختار أيضاً أن يوجهك نورتون كلما توفرت عمليات التحديث لتطبيقها على الكمبيوتر تلقائياً. وإذا كنت تفضل الحصول على عمليات التحديث الحديثة لوحدك، يمكنك أن تنقر على الزر Live Update في أعلى شاشة بدء البرنامج لكي تحمّل عمليات التحــديث بشكل يدوي. وتقدم الحزم البرمجية AV الأخرى آليات مشابهة من أجل التحديث التلقائي.

إذا لم يكن التحديث التلقائي متوفراً لبرمجياتك AV المختارة (وهذا الاحتمال مستبعد)، يجب أن تحصل على الأقل على تعليمات واضحة بشأن موقع الوب لإجراء عمليات التحميل.

يمكنك حماية نفسك أيضاً من برامج مالوير بالمحافظة على تحديث البرمجيات الأخــرى، وخصوصاً نظام التشغيل والتطبيقات الأخرى مثل إنترنت إكسبلورر. يقدم الفصــل الســابع مزيداً من التفاصيل عن طريقة تحديث هذه البرمجيات.

4-5 ما الذي تفعله إذا ظهر لديك فيروس أو دودة

يظل احتمال إصابة كمبيوترك قائماً، حتى لو كانت وسائل دفاعك على أهبة الاستعداد. لكن الإصابة ليست مبرراً لحدوث الفزع. ويمكن أن تتعافى، وفي بعض الأحيان بسهولة كبيرة، من هجوم الفيروس أو الدودة.

كيف تعرف بأن كمبيوترك مصاباً

إن الطريقة الأفضل لكي تعرف بإصابة كمبيوترك هي تشغيل عمليات المسح AV بشكل دوري وباستخدام التواقيع الحديثة. يمكنك أن تطلب مسح كمبيوترك عبر الإنترنت. على سبيل المثال، يمسح Symantec Security Check كمبيوترك عبر الإنترنت بحثاً عن الفيروسات وبرامج مالوير الأخرى. لكي تشغل مسح مجاني، اذهب إلى www.symantec.com/avcenter. وانقر الرمز Check for Security Risks في أسفل الصفحة.

توجد خدمات مجانية مشابهة من بائعي البرمجيات AV الآخرين. ففي الموقع www.mcafee.com، يمكنك أن تنقر على الارتباط Home and Home Office وتبحث عن المربع Free Tools على الجانب الأيسر من صفحة البدء. وفي الموقع www.trendmicro.com، يمكنك أن تنقر على الارتباط Personal. يوجد الارتباط Trend Micro House Call في أعلى الصفحة. يبدأ هذا الارتباط مسح مجاني للفيروسات. وتقدم الشركة Panda Software أداة مسح مجانية في الموقع http://www.pandasoftware.com/activescan/com/activescan_principal.htm.

على كل حال، قد لا يكشف المسح برامج مالوير الجديدة التي لا يوجد توقيع عنها بعد. لذلك راقب الإشارات التي قد تدل على إصابة. على سبيل المثال، هل يوجد ملفات مخربة أو مفقودة أو هل تغيرت بعض إعدادات التطبيقات أو تم إلغاء تأهيل البرمجيات الأمنية؟ هل أصبح كمبيوترك بطيئاً فجأة أو يتصرف بشكل مزعج؟ هل يكشف جدار النار البرامج التي لم تفتحها لتحاول الوصول إلى الإنترنت؟ هذه هي جميع الإشارات التي تدل على وجود مشكلة.

كيف تزيل دودة أو فيروس

بعد أن تكتشف فيروس على كمبيوترك، يمكنك تشغيل البرمجيات AV لإزالته. وبعد أن ينتهي المسح، يجب أن توجهك البرمجيات لإزالة أو حجر أي فيروس تم اكتشافه. (يعني حجر برنامج مالوير أن تتركه على كمبيوترك ولكن بحالة معزولة لا يمكنه أن يسبب أذية). ويمكن أن تنظف البرمجيات AV أيضاً الملفات المصابة بفيروس.

يقدم بائع البرمجيات AV أيضاً أدوات خاصة لإزالة الديدان ومالوير مثل أحصنة طروادة (يتم تغطيتها بمزيد من التفصيل في الفصل الخامس). يمكنك أن تحمّل هذه الأدوات من موقع وب البائع AV. يجب أن تنصح البرمجيات AV بضرورة استخدام أداة ضرورية إذا لزم الأمر. وفي الشريط الجانبي "إزالة إصدار الدودة Beagle" أشرح الخطوات التي نفذتها لإزالة الدودة التي أصابت كمبيوتري.

في سيناريو الحالة الأسوأ، لا تستطيع البرمجيات AV أن تزيل مالوير. وقد تحتاج عند

ذلك إلى مساعدة خارجية. اتصل بخدمة دعم الزبائن لبائع البرمجيات AV لكي تعـــرف مـــا يوصي به (لكن استعد لانتظار طويل). يمكنك أن تتصل أيضاً بمصنّع الكمبيـــوتر، وتطلـــب المساعدة من المخزن الذي اشتريت منه الكمبيوتر (لقاء أجرة) أو من مخزن صيانة كمبيوترات محلي.

وكحل أخير، يمكنك أن تبدأ من جديد وتعيد تثبيت نظـــام التشـــغيل والتطبيقـــات باستخدام أقراص البرمجيات الأصلية. لكي تؤدي ذلك أدخل قرص نظام التشغيل الأصـــلي في محرك الأقراص المضغوطة وأعد تشغيل الكمبيوتر. يطلب منك الكمبيوتر التأكد على رغبتـــك بإعادة تثبيت نظام التشغيل. على كل حال، تؤدي إعادة تثبيت نظام التشغيل إلى مسح جميع البيانات التي حفظتها على كمبيوترك (لنفترض أنك تقوم بعمليات النسخ الاحتياطي بشـــكل دوري). تأكد من تنفيذ جميع الخيارات قبل إعادة فرز وتنسيق محرك القرص الصلب.

6-4 اختيار برمجيات مضادة للفيروسات

إذا لم يكن لديك برمجيات مضادة للفيروسات، فيوجد أمامك عدد كبير من الخيارات. الشركات الثلاثة الكبار هي Symantec، التي تبيـــع Norton AntiVirus؛ Trend Micro التي تبيع PC-cillin؛ وMcAfee التي تبيع VirusScan.

إن فوائد اختيار حل من إحدى الشركات الثلاثة الكبيرة هي أنها تملك مجموعات بحث جيدة تنتج تواقيع الفيروسات بشكل فوري، وتملك البنية التحتية لتوزيع إجراءات التحديث إلى زبائنها. أما سيئة هذا الاختيار فهي أنه الأغلى.

هناك عدة شركات أخرى تقدم أيضاً منتجات جيدة. وتضم Computer Associates، Kaspersky Lab، F-Secure، ZoneLabs، ESET وPanda Software.

يمكنك أيضاً أن تحصل على برمجيات مضادة للفيروسات مجانية مـــن شـــركة تـــدعى GriSoft. ويقدم منتجها المضاد للفيروسات AVG جميع المزايا العامة للمنتجات غير المجانية. فهو يمسح الملفات والبرامج الجديدة والبريد الإلكتروني ويسمح بتشغيل مسح القرص الصلب الكامل. ويقدم أيضاً أدوات خاصة لإزالة الفيروسات بالإضافة إلى عمليات التحديث التلقائي لتواقيع الفيروسات الجديدة. السيئة الوحيدة هي أن مستخدمي الإصدار الجديد لا يتلقون أي دعم تقني. إذا كنت مستخدم مسجل، يمكنك أن تضع أسئلة لكي يراها مســـتخدمو AVG الخبراء في المنتدى على الوب، ولكن لا يمكنك مخاطبة قسم الدعم التقني بالبريد الإلكتروني أو الهاتف ما لم تشتري الإصدار المدفوع. (على كل حال، ثمن البرمجيات المدفوعة أقل بكثير من معظم المنتجات AV).

بشكل عام، تقدم جميع المنتجات مستوى أمني متماثل. فالعديد من الشركات تقدم فترة تجريبية مجانية، فيمكنك اختبار عدة برامج. وتعتبر هذه فكرة جيدة، لأنه يمكنك التعرف على

البرنامج الذي يقدم واجهة المستخدم الأفضل ويقدم المستندات الأفضل على الـوب. يـذكر الجدول 4-3 شركات البرمجيات المضادة للفيروسات، مواقع الوب التي تقـدم الإصـدارات التجريبية أو التي تبيع المنتج. لقد كانت تتراوح الأسعار في منتصف عام 2005 مـن 24.95$ إلى 49.95$ للبرمجيات المضادة للفيروسات، ولكن يوجد عروض خاصـة وتتـوفر إمكانيـة المساومة. كما ذكرنا سابقاً، سوف تستفيد بشكل أكبر من المنتج الذي يقدم الوظائف الأمنية الأخرى بالإضافة إلى الحماية من الفيروسات.

الجدول (4-3):

المنتجات الأساسية المضادة للفيروسات		
المنتج	**البائع**	**موقع الوب**
Anti-Virus Personal	Kaspersky Lab	www.kaspersky.com
AVG AntiVirus	Gri Soft	http://free.grisoft.com
eTrust Antivirus	Compute Associates	www.ca.com
F-Secure Antivirus	F-Secure	www.f-secure.com
NOD32	ESET	www.eset.com
Norton AntiVirus	Symantec	www.symantec.com
PC-cillin	Trend Micro	www.trendmicro.com
Titanium Antivirus	Panda Software	www.pandasoftware.com
VirusScan	McAfee	www.mcafee.com
ZoneAlarm AntiVirus	Zone Labs	www.zonelabs.com

إذا كنت ترغـب بمزيـد مـن النصـائح، فـإن المجـلات ومواقـع الـوب مثـل PC Magazine (www.pcmagazine.com)، PC World (www.pcworld.com)، وCNET (www.cnet.com.) تراجع بشكل دوري المنتجات للأمنية وتقدم عادةً "اختيـار المحرر". يمكنك أن تقرأ هذه المراجعات وتقارن بين الأسعار والمزايا على هذه المواقع.

4-7 لائحة التدقيق

استخدم هذه اللائحة كدليل مرجعي للمواد المغطاة في هذا الفصل.

ما يجب أن تفعله

- استخدام البرمجيات المضادة للفيروسات، سواء كانت برمجيات مستقلة أو جزء من حزمة.
- إنجاز عمليات المسح لكمبيوترك بشكل دوري، والمحافظة على تحديث البرمجيات المضـادة للفيروسات.

- حافظ على تحديث برمجيات نظام التشغيل وبرنامج الاستعراض.
- أنجز عمليات نسخ احتياطي للملفات الأساسية بشكل دوري.

ما يجب أن لا تفعله

- فتح البريد الإلكتروني المشتبه به وغير المطلوب ومن أشخاص لا تعرفهم.
- نقر الارتباطات ضمن رسالة البريد الإلكتروني أو فتح الملفات المرتبطة من الغرباء.

8-4 موارد مساعدة

يقدم هذا القسم موارد إضافية لمساعدتك على تعلم المزيد. وتقدم جميع شركات AV الواردة في هذا الفصل معلومات عن ظهور الفيروسات، عمليات تحديث AV المؤخرة، وأدوات الإزالة. وتقدم نصائح لتجنب الإصابة ببرامج مالوير وتأمين كمبيوترك.

وتعتبر اللائحة Virus List في الموقع www.viruslist.com التي تقدمها شركة البرمجيات المضادة للفيروسات Kaspersky Lab، مورداً ممتازاً للحصول على معلومات عن المالوير، السبام، المهاجمون الخبيثون وقضايا أمن الإنترنت العامة. يقدم هذا الموقع موسوعة بمواضيع مالوير ونصائح لمساعدتك في تأمين كمبيوترك بشكل أفضل.

ويقدم Virus Bulletin في الموقع www.virusbtn.com، معلومات كثيرة عن الفيروسات والمالوير. ويبيع أيضاً رسائل إخبارية مع معلومات من مجتمع بحث البرمجيات المضادة للفيروسات.

تعتبر الشركة WildList، في الموقع www.wildlist.org، نفسها مدققة لباعة البرمجيات المضادة للفيروسات، الذين قد يضخمون عدد الفيروسات الموجودة فعلاً. فحسب البائع الذي تختاره يتراوح مقدار الفيروسات من 50000 إلى 90000 والرقم في تصاعد. على كل حال، عدد الفيروسات التي تملك القدرة على الانتشار أقل بشكل ملحوظ.

تتعقب هذه الشركة الفيروسات التي تؤثر على الكمبيوتر العادي أثناء الاستخدام اليومي. وتختلف الفيروسات التي تصيب الكمبيوترات عن الفيروسات التي يتم اكتشافها في المختبر من الباحثين أو التي يتم إصدارها كدليل عن مفهوم بدون إطلاقها عملياً. تعتمد WildList على المتطوعين من مجتمع أبحاث البرمجيات المضادة للفيروسات وغيره للمساهمة في عينات من الفيروسات وتعقب الفيروسات في بيئة الكمبيوترات العالمية.

إزالة إصدار الدودة Beagle

في أواخر كانون الثاني 2005، أصيب كمبيوتري بإصدار من الدودة Beagle يدعى Beagle.BA (تدعوها معظم البرمجيات AV الدودة Bagle)، وهو إصدار جديد من مالوير قديم. يتم إنشاء هذه الإصدارات الجديدة عندما يأخذ مبرمجو المالوير فيروس أو دودة موجودة ويجرون تعديلات وإضافات على البرمجيات. إن الدودة Beagle.BA هي دودة ترسل البريد بأعداد كبيرة وحاولت أيضاً أن تغلق البرمجيات المضادة للفيروسات والبرمجيات الأمنية التي تعمل على كمبيوتر المضيف. وهي تقنية شائعة لدى الديدان، خصوصاً الديدان التي تحاول إدخال حصان طروادة إلى الكمبيوتر فيمكن أن يستخدمه المهاجم لاحقاً. ومن حسن حظي أن Beagle.BA لم يحمل حصان طروادة في برمجياته.

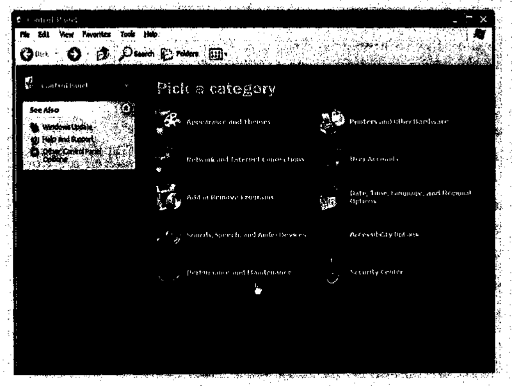
لقد اكتشفت بأن كمبيوتري مصاب عندما كشف مسح القرص الصلب الدوري الدودة. وحذفت البرمجيات Norton AntiVirus الدودة من كمبيوتري، ولكن يوصي أيضاً بتحميل أداة إصلاح خاصة لتصحيح ما خربته الدودة عندما ثبتت نفسها على كمبيوتري.

ذهبت إلى www.symantec.com ونقرت الارتباط Security Response، الذي أخذني إلى صفحة البدء Security Response. وفي هذا الوقت كان إصدار Beagle.BA ما يزال مذكوراً على الصفحة الأولى من Security Response، لذلك نقرت الارتباط، الذي أخذني مباشرة إلى أداة إزالة Beagle.BA. (إذا لم يمكنك العثور على فيروس محدد على الصفحة الأولى من Security Response، يمكنك أن تدخل الاسم في حقل البحث لكي تجد الصفحة المناسبة).

توصي التعليمات الموجودة على صفحة الوب أن ألغي تأهيل System Restore، وهي وظيفة في ويندوز تراقب التغييرات الطارئة على ملفات النظام الأساسية والمسجلات التي تسمح لنظام التشغيل بالعمل. يمكنك أن تستخدم System Restore لأخذ لقطة عن حالة جيدة ومعروفة عندما يكون كمبيوتري في حالة عمل نظامية. إذا قاطع شيء ما العمل النظامي، يمكنك أن تستخدم System Restore لتعيد حالة جيدة معروفة.

على كل حال، تحفظ برامج المالوير نفسها غالباً في ملفات النظام والمسجلات، لذلك فمن المحتمل أن تحفظ الميزة System Restore دودة أو فيروس وتعيد تثبيت البرنامج مالوير على كمبيوترك. وبإلغاء تأهيل System Restore، تزيل جميع نقاط الحفظ السابقة التي حفظها في هذا المكان. لكي تتعلم المزيد عن System Restore، انقر Start، انقر الزر Help and Support، واكتب System Restore overview في حقل البحث.

إن إلغاء تأهيل System Restore بشكل مؤقت لا يؤثر على ملفاتك الشخصــية، مثل مستندات وورد، الصــور وملفــات الوســائط المتعــددة. لكــي تلغــي تأهيــل System Restore، انقر Start، ثم حدد Control Panel. (حسب طريقة إعداد القائمة Start، قد تحتاج إلى نقر Settings لكي تجد الخيــار Control Panel). عنــدما تنقــر Control Panel، تفتح نافذة تقول Pick a category "حدد فئة"، كما هــو مــبين في الشكل 4-1.



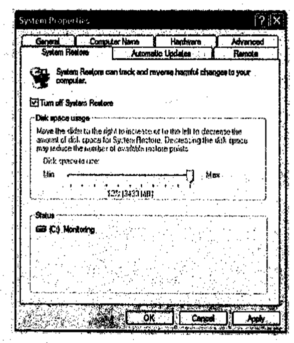
الشكل (4-1): فئة الأداء والصيانة في Control Panel.

اختر الفئة Performance and Maintenance، ثم انقر System option، كما هو مبين في الشكل 4-2. يظهر إطار صغير بعنوان System Properties، كما هو مــبين في الشكل 4-3. يوجد في هذا الإطار عدة أبــواب، مثــل General، Computer Name وHardware. حدد علامة التبويب System Restore. فترى مربع تدقيق يدعى Turn Off System Restore. دقق المربع وانقر الزر Apply في أسفل الإطار.

بعد ذلك أحمّل الأداة، تدعى FxBeagle، وأشغلها على كمبيوتري. عندما تنتــهي الأداة، أعود إلى الإطار System Restore وأعيد تأهيل System Restore. وبعد ذلــك أطلب مسح كامل القرص مرة أخرى لكي أضمن أن كمبيوتري نظيفاً.



الشكل (2-4): الفئة System في فئة الأداء والصيانة.



الشكل (3-4): مربع حوار خصائص النظام.

إذا كنت واثقاً أن كمبيوترك نظيف، يمكنك أن تعدّ نقطة حفظ. لكي تعدّ نقطة حفظ، انقر Start، ثم اختر All Programs، Accessories، System Tools، وSystem Restore. فيقودك معالج عبر الخطوات الضرورية لإعداد نقاط الحفظ.

الفصل الخامس

التخلص من الضيوف غير المرغوبين، الجزء 2: سبايوير، أدوير وأحصنة طروادة

بحث الفصل السابق في نمو برامج المالوير واختبر صنفين منها: الفيروسات والديدان. ويبحث هذا الفصل ثلاثة أنواع مميزة من التهديدات الأمنية: سبايوير، أدوير وأحصنة طروادة. سوف نعرّف كل من هذه المخاطر، ونتحدث عن التحديات القانونية والتقنية للتعامل مع سبايوير وأدوير، ثم نبحث طرق الحماية من هذه التحديات.

1-5 ما هي سبايوير، أدوير وأحصنة طروادة؟

بالمعنى الضيق، سبايوير هي مصطلح لتقنيات التعقب (خصوصاً، التطبيقات التنفيذية) التي يتم تثبيتها على كمبيوترك بدون أن تلاحظ ذلك، بدون موافقتك أو بدون أن تتحكم بها. يمكن أن تراقب سبايوير نشاطاتك على الوب وتؤدي وظائف بدون معرفتك أو موافقتك. وحسب البرنامج فإن سبايوير يمكن أن تتعقب وتصدر تقريراً عن كل موقع تزوره، تولد الإعلانات المنبثقة، تغيّر صفحة البدء وإعدادات برنامج الاستعراض أو تسجل كل مفتاح تضغطه. وبالمعنى الأوسع، يتم استخدام سبايوير بشكل واسع كاسم شامل لمعظم أنواع التقنيات غير المرغوبة التي تكشفها البرامج المضادة للسبايوير الشائعة. ويتم تنفيذ هذه التقنيات بطرق تقلل من تحكمك بما يلي: تجميع، استخدام وتوزيع المعلومات الشخصية؛ التغييرات المادية التي تصيب خصوصيتك وأمن النظام؛ واستخدام موارد النظام. وهذه البرامج هي التي يرغب المستخدمون أن تكشفها البرمجيات المضادة للسبايوير ويريدون إزالتها أو توقيفها بأسهل طريقة.

أدوير هي مجموعة من فئة سبايوير الأوسع، وهي مصممة لتسليم الإعلانات الموجهة إلى

برنامج استعراض الوب، وخصوصاً باستخدام الإعلانات المنبثقة. يتم غالباً حزم أدوير مع برمجيات أخرى، مثل برمجيات مشاركة الملفات ند لند، الألعاب أو الأدوات الأخرى التي يمكن تحميلها مجاناً من الوب. تعرف أدوير أي نوع من الإعلانات تعرضه على كمبيوترك لأنها تتعقب المواقع التي تجول إليها. على سبيل المثال، إذا تجولت إلى موقع تأجير سيارات، قد يولد برنامج أدوير إعلان منبثق دفعت شركة تأجير سيارات منافسة نقوداً إلى شركة الأدوير لكي تعرضه عليك. وبالإضافة إلى تعقب حركاتك وإزعاجك بالإعلانات، يمكن أن تفتح أدوير وصلة على الإنترنت لكي ترسل تقريراً عن أسلوبك في التجول إلى ملقم مركزي. تضم هذه المعلومات عمرك، جنسك، عادات التسوق لديك وحتى موقعك ويتم استخدامها لإجراء عمليات "بحث السوق" وجذب زبائن جدد.

أما أحصنة طروادة فهي برامج تدعي بأنها برامج أخرى. على سبيل المثال، قد يبين حصان طروادة أنه مقطوعة محركة مسلية، شاشة توقف أو برنامج مجاني يقوم بشيء مفيد. لكن أحصنة طروادة تؤدي وظائف غير معلنة (إذا كانت الوظائف المعلنة حقيقية أصلاً). إن الهدف الأقصى من حصان طروادة هي تثبيت باب خلفي في كمبيوترك أو سرقة كلمات المرور. يسمح الباب الخلفي للمهاجمين بالتحكم بكمبيوترك عن بعد. ويمكن اعتبار بعض أنواع السبايوير بأنها أحصنة طروادة لأنها تصل بحجة مضللة. على سبيل المثال، قد تحمّل شاشة توقف أنيقة مع فراشات جميلة فيحدث أنها تراقب عاداتك في التجول على الوب أو تسجل ضربات المفاتيح. وتعتمد أحصنة طروادة غالباً على الفيروسات، الديدان والهندسة الاجتماعية لكي تجذب المستخدمين إلى تحميلها.

لقد أصبح مصطلح حصان طروادة مستخدماً لوصف أي برنامج يوجد على كمبيوترك ويقدم الوصول عن بعد إلى شخص غير مرخص أو يؤدي وظائف غير مرغوبة. وتكشف معظم البرمجيات المضادة للفيروسات (AV) وبعض البرمجيات المضادة للسبايوير أحصنة طروادة.

لا تستطيع سبايوير، أدوير وأحصنة طروادة أن تنسخ نفسها. ولذلك تحتاج هذه التطبيقات إلى طرق أخرى من أجل الانتشار. على سبيل المثال، يمكن تسليم أحصنة طروادة مع دودة أو فيروس، كملف مرتبط مع رسالة إلكترونية أو في حزمة مع برمجيات أخرى. وتستخدم سبايوير وأدوير تقنيات مشابهة للانتشار، ولكن يتم تحميلها غالباً كجزء من برنامج مجاني لمشاركة الملفات أو أداة برمجية أو تحميل الملفات أثناء التجول على الوب بدون إذنك.

تعريف سبايوير وأدوير

يوجد فروق كبيرة بين سبايوير وأدوير وبين الفيروسات من حيث الحكم عليها كبرامج

مطلوبة أو غير مطلوبة وما إذا كنت تريدها على كمبيوترك، مع أنه يمكن النظر إلى مخاطرها الأمنية كامتداد لمشكلة الفيروسات. الفيروسات، الديدان، وأحصنة طروادة هي برمجيات غير مرغوبة دوماً ويجب إزالتها تلقائياً من كمبيوترك. فالعديد من البرامج المصنفة كأدوير وسبايوير عالية الخطورة وتؤثر بشكل سلبي بالغ على أداء كمبيوترك أو تنتهك خصوصيتك بإرسال معلومات شخصية إلى جهة أخرى.

على كل حال، برامج أدوير الأخرى ذات حدّ أدنى من الخطورة. فهي تنقل الوظائف المفيدة مثل الألعاب أو الأدوات ولها تأثير منخفض على أداء الكمبيوتر وانتهاك الخصوصية. وكما أن برامج البث التلفزيوني مجانية لأن شركات التلفزيون تحقق عائداً من الإعلانات، فإن العديد من البرامج مجانية لأنها تعتمد على الإعلانات لتحقيق الربح، وتدعى برامج مدعومة بالإعلانات، فتتضمن أدوير لكي تنقل الإعلانات. وتطلب بعض البرامج المدعومة بالإعلانات موافقة المستخدم قبل تثبيت أدوير؛ وبعضها الآخر لا يطلب موافقة المستخدم. ويستمر بعض منها بالعمل في المنطقة الرمادية حيث تكون موافقة المستخدم جزء من اتفاقية استخدام البرمجيات. سوف نبحث هذه الفروق وما تعنيه بالنسبة لك في الأقسام التالية.

يمكن تقسيم الطيف العريض من سبايوير وأدوير أو البرامج غير المرغوبة إلى فئتين عامتين: برامج عالية الخطورة أو خبيثة وبرامج منخفضة الخطورة. يسند الباحثون الأمنيون برامج سبايوير وأدوير إلى إحدى هاتين الفئتين حسب طريقة تثبيت هذه البرامج، نوع البيانات التي تحاول إرسالها من الكمبيوتر، تأثيرها على أداء الكمبيوتر، وما الذي تبينه عن عملها وقصدها. عندما يتحرى الباحثون الأمنيون سلوك برنامج لكي يحددوا خطورته، يدققون عدداً من النواحي الأساسية وتشمل مميزات التثبيت، خصائص العمل الصامت، انتهاك الخصوصية، التأثير على تكامل البرامج، التأثير على أداء الكمبيوتر وسهولة إزالتها:

- هل يؤثر البرنامج على استقرار النظام أو أنه يبطئ وصلة الشبكة؟
- هل يطلق البرنامج إعلانات منبثقة؟ إذا كان الأمر كذلك، كم مرة؟
- هل يخدم البرنامج كوسيلة لتحميل وتثبيت برامج أخرى تحمل أخطار أمنية (مثل سبايوير إضافي و/أو أدوير)؟
- هل يستبدل برنامج الاستعراض صفحة البدء أو يغير خيارات أو سلوك البحث؟
- هل يسبب البرنامج إنشاء معلومات سرية وحساسة مثل أرقام الحساب المصرفية وكلمات المرور؟
- هل يسبب البرنامج إصدار بيانات أقل حساسية مثل تعقب أسلوب التحول على الوب؟

- هل يملك البرنامج سياسة خصوصية، وهل يتطابق سـلوكه مـع السياسـة المصـرح عنها؟
- هل يحاول البرنامج إخفاء نفسه أو يتجنب إزالة التثبيت عندما يحاول المستخدم ذلك، بما في ذلك إعادة التثبيت والتقنيات غير المرغوبة لإعادة تشغيل العمليـات الـتي أوقفهـا المستخدم؟
- هل يفتقد البرنامج إلى ميزة إزالة التثبيت أو يفشل بالتسجيل في ميزة إضـافة أو إزالـة البرامج في مايكروسوفت ويندوز؟
- هل يثبت البرنامج نفسه بصمت؛ وبدون أي إشارة إلى المستخدم؟
- هل يفتقد البرنامج واجهة مستخدم؟
- هل يحجب البرنامج عملياته أو يخفيها عن المستخدم تحت اسم غامض؟
- هل يتم إعلام المستخدم عن وجود البرنامج عبر اتفاقية تصريح المستخدم (EULA)؟ هل يظهر أن EULA تتعلق ببرنامج مختلف؟

لكي تصنف البرامج سبايوير وأدوير كعالية الخطورة أو خبيثة، يجب أن تملـك هـذه البرامج تأثير كبير على استقرار النظام و/أو أدائه أو أنها تفشي معلومات سرية وحساسة و/أو تتصرف خلسةً مثل التثبيت الصامت، عدم تقديم واجهة مستخدم، وحجب عمليات التطبيق. تشمل الأمثلة عن البرامج عالية الخطورة مسجلات ضربات المفاتيح، قرصنة برامج الاستعراض، وطلب الاتصال الهاتفي. (يبين الجدول 5-1 هذه البرامج وأنواع أخرى. إن سبايوير الخبيـث غير قانوني لذلك يتم توظيفه من المجرمين الذين يريدون سرقة معلومات منك. يـتم تثبيـت سبايوير الخبيث على كمبيوتر باستغلال خلل في البرمجيات، الديدان والفيروسات، الهندسـة الاجتماعية والتحميل بالتجول على الوب.

تضم البرامج منخفضة الخطورة العديد من أدوير التجاري أو البرامج المساعدة للإعلانات الشائعة. وتولد بعض الأدوير إعلانات منبثقة متعددة وتنجز وظائف غير مرغوبة أخرى، مثل تغيير صفحة البدء، توجيهك إلى محركات بحث غير مألوفة أو تثبيت أشرطة أدوات في برنامج الاستعراض لم تطلبها ولا تريدها. ويمكن أن تقرأ أدوير أيضاً الكعكات المثبتة في كمبيـوترك لكي تحصل على معلومات عنك وعن سلوكك في التجول على الوب.

وبغض النظر عما إذا كان البرنامج عالي أو منخفض الخطورة، فإن المستخدم يجـب أن يملك التحكم المطلق بجميع البرامج الموجودة على كمبيوتره، بما في ذلك القدرة على البحـث عن البرامج التي لا يريدها وإزالتها. وكما سترى في القسم التالي فإن بعض بـرامج سـبايوير وأدوير تحاول انتزاع قدرتك على التحكم بذلك.

الجدول (5-1):

تعاريف السبايوير	
المصطلح	**التعريف**
سبايوير	سبايوير هو فئة عامة من البرمجيات التي تراقب نشاط الكمبيوتر وترسل تلك المعلومات إلى كمبيوترات أو مواقع أخرى على الإنترنت. وتشمل المعلومات التي تجمعها وترسلها سبايوير كلمات المرور، تفاصيل تسجيل الدخول، أرقام الحسابات، المعلومات الشخصية، الملفات المنفردة، والمستندات الشخصية. ويمكن أن تجمّع سبايوير أيضاً وتوزع معلومات متعلقة بكمبيوتر المستخدم، معلومات عن التطبيقات التي تعمل على الكمبيوتر، استخدام برنامج استعراض الإنترنت، وغيرها من النشاطات الكمبيوترية. يتم تحميل سبايوير عادةً في كمبيوتر المستخدم بدون علمه، ويكتب برمجياته المهاجمون والمجرمون.
أدوير	أدوير هو نوع من تقنية العرض الإعلاني – خصوصاً، التطبيقات التنفيذية والتي تهدف بشكل رئيسي لتسليم المحتوى الإعلاني. تؤدي العديد من تطبيقات أدوير وظائف التعقب أيضاً ولذلك يمكن تصنيفها كتقنيات تعقب. قد يرغب المستخدمون بإزالة أدوير إذا كان يعترضون على هذا التعقب، لا يرغبون برؤية الإعلانات التي يولدها البرنامج أو أنهم مستاؤون من تأثيره على أداء النظام. وقد يرغب بعض المستخدمين بالاحتفاظ ببرامج أدوير معينة إذا كان وجودها هو شرطاً لاستخدام برمجيات مجانية أخرى. يتم إنشاء أدوير في شركات البرمجة التجارية وليس من قبل المجرمين، ويتم حزمها مع برمجيات مجانية غالباً، مثل برامج مشاركة الملفات. تشرح بعض برامج الأدوير وظائفها في اتفاقية تصريح الاستخدام وتقدم خيارات إزالة التثبيت؛ كما تثبت برامج أدوير الأخرى نفسها بدون إذن المستخدم وتقاوم محاولات إزالتها.
مسجل ضربات المفاتيح	تقنيات تعقب تقوم بتسجيل ضربات لوحة المفاتيح خلسةً. وهي إما أن تسجل ضربات المفاتيح من أجل استردادها لاحقاً أو لإرسالها عبر البريد الإلكتروني إلى شخص بعيد يشغل هذا المسجل. يتم استخدام مسجلات ضربات المفاتيح لسرقة كلمات المرور ومعلومات الهوية الأخرى.

تعاريف السبايوير

المصطلح	التعريف
قرصان برنامج الاستعراض	تغير قراصنة برامج الاستعراض صفحة البدء وتعيد توجيه برنامج الاستعراض إلى محركات بحث غير مرغوبة أو غير معروفة أو إلى مواقع وب أخرى. ويمكن أن يمنعك بعض قراصنة برنامج الاستعراض من استعادة صفحة البدء التي تريدها. تعمل قراصنة برامج الاستعراض بحذف إدخال صفحة البدء الذي حددته وإدخال عنوانهم في ملف خاص يستشيره الكمبيوتر (ملف المضيف). وقد تعترض أيضاً استعلامات البحث المكتوبة في محرك بحث نظامي وتعرض نتائج خاصة بها.
كائن مساعد برنامج الاستعراض (BHO)	تطبيق مرافق لمستكشف إنترنت مايكروسوفت (IE) يعمل بشكل تلقائي عند تشغيل IE. إنه نوع من أدوات الإدارة. ويتم تنفيذ العديد من تقنيات التعقب أو تقنيات العرض الإعلاني باستخدام BHO. كما يمكنه البحث في صفحات الوب عندما يزورها المستخدم واستبدال الملصقات الدعائية التي يولدها ملقم الوب بالإعلانات المستهدفة. ويمكنه مراقبة وإصدار تقارير عن سلوك المستخدم في التجول على الوب، وقد يغير صفحة البدء. لاحظ أنه ليست جميع التطبيقات BHO خبيثة؛ فالعديد من أشرطة أدوات برامج الاستعراض النظامية هي BHO.
حصان طروادة	برمجيات تتظاهر بأنها مفيدة لتخدع المستخدم وتغريه بتثبيتها، وبعد تثبيتها تبدأ بتنفيذ وظائفها غير المرغوبة وغير المعلنة.
الوصول عن بعد/أداة الإدارة (RAT)	تطبيقات تنفيذية مصممة للسماح بالوصول عن بعد إلى النظام والتحكم به. فهي نوع من تقنية التحكم عن بعد. ولا تسبب العديد من الاستخدامات النظامية للتطبيقات RAT تهديداً أمنياً، ولكن يمكن استخدامها بشكل خبيث، وخصوصاً عند استخدامها من قبل شخص آخر غير مالك الكمبيوتر النظامي.
طالب الاتصال الهاتفي	برامج تستخدم مودم الكمبيوتر لإجراء اتصالات أو الوصول إلى خدمات. قد يريد المستخدمون أن يزيلوا طالبات الاتصال الهاتفي فيؤدي إلى الاتصال بأرقام غير متوقعة وإلى تحمل كلفة الاتصال الهاتفي. وطالب الاتصال الهاتفي هو مصطلح عامي لتقنية الاتصال الهاتفي.

2-5 التحديات التقنية والقانونية لكشف وإزالة سبايوير وأدوير

تحدث الفصل الرابع، "التخلص من الضيوف غير المرغوبين، الجزء 1: الفيروسات والديدان" عن الأسباب المختلفة لنمو برامج المالوير (سهولة الاتصال، بيئة الكمبيوترات المتجانسة، استجابة البرمجيات الأمنية). تؤدي العوامل نفسها إلى نمو برامج سبايوير، لكن سبب وجود سبايوير وأدوير الذي لا ينكر هو المال. سواء كان الأمر يتعلق بتسهيل سرقة الهوية، تجنيد كمبيوترك وتأجيره في عمليات على الشبكة أو توليد عائداً إعلانياً لشركات البرمجة المشبوهة، فإن هذا النوع من التطبيقات يتأثر بشكل متزايد بالمردود المادي. والأرباح الهائلة التي يمكن توليدها من سبايوير وأدوير تجعلها مشكلة صعبة الحل. فيمكن لسماسرة سبايوير تشغيل المبرمجين لتعديل الشيفرة باستمرار من أجل تجنب كشفها وإزالتها بالبرمجيات الأمنية أو التشجيع على تطوير برامج المصادر المفتوحة أو المكتبات الاحترافية.

كم تبلغ الأرباح التي يحققها هذا النوع من البرمجة؟ انظر إلى هذه القصة: ربحت شركة أدوير تدعى كلاريا حوالي 90 مليون دولار في 2003. (منتجات أدوير من كلاريا معروفة باسم GAIN أو Gator، وتأتي غالباً في حزمة مع برمجيات أخرى من Kazaa، برمجيات ند إلى ند). وبهذا القدر من الأرباح يتوفر لدى الشركة دافع قوي للاستمرار في هذا العمل. ومن شركات أدوير الأخرى .WhenU، 180Solutions، Avenue Media وDirect Revenue.

وتبين العديد من المؤشرات الأثر العميق لسبايوير وأدوير. أجرى مزود خدمة الإنترنت Earthlink (ISP) دراسة مع WebRoot التي تنتج البرمجيات المضادة للسبايوير. مسحوا أكثر من 3.2 مليون كمبيوتر ووجدوا 26 برنامج سبايوير على كل كمبيوتر بشكل وسطي. تقول شركة Dell Computer أن مشاكل سبايوير هي السبب الأول لاتصالات الدعم التقني. وأجرت Symantec دراسة لترى أي فئات من مواقع الوب تخلّف أكثر البرمجيات غير المرغوبة. أخذ الباحثون كمبيوتر ويندوز جديد ووصلوه إلى الإنترنت بدون أي برمجيات حماية عادية واستعرضوا الإنترنت. واستغرق كل من الباحثين ساعة من الزمن كلاً منهم بالتحول إلى الفئات المختلفة من مواقع الوب. وللمفاجأة خلّفت مواقع الوب الخاصة بالأطفال أكثر البرمجيات غير المرغوبة على الكمبيوتر – 359 برنامج أدوير خلال ساعة واحدة من التحول على الوب. وللمقارنة فإن الرقم الأعلى التالي كان 64 برنامج أدوير تم تثبيتها من مواقع وكالات السفر. أما مواقع الألعاب فقد خلّفت أربعة برامج. يسرد الجدول 5-2 النتائج الكاملة.

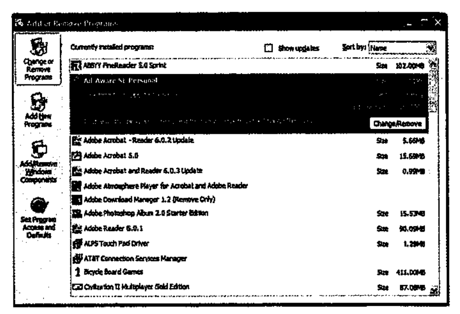
الجدول (5-2):

دراسة Symantec حول "البرمجيات غير المرغوبة"				
فئة الموقع	أدوير	سبايوير	قراصنة	كعكات
ألعاب	23	4	2	68
أطفال	359	0	3	31
أخبار	3	1	0	26
إعادة بيع	2	1	1	22
تسوق	0	0	0	10
رياضة	17	2	0	72
سفر	64	2	1	35

يميل مبرمجو أدوير وسبايوير عالية الخطورة إلى جعل البحث عن برمجياتهم والتخلص منها أمر صعب. على سبيل المثال، قد يضع برنامج سبايوير آلاف الملفات على كمبيوتر ويجري آلاف التغييرات على المسجل Registry. والمسجل هو قاعدة بيانات بالإعدادات تخبر الكمبيوتر عن التطبيقات وملفات المستخدمين الموجودة على كمبيوترك. يعود الكمبيوتر إلى المسجل عند الإقلاع وعندما يفتح البرامج. تقحم السبايوير وأدوير نفسها في المسجل لتصبح أحد البرامج التي يشغلها الكمبيوتر تلقائياً.

قد تصنع سبايوير وأدوير نسختين عن نفسها على كمبيوترك فإذا حذفت إحدى النسختين، يستمر تشغيل النسخة الاحتياطية. أو قد تزرع "مسربات" على كمبيوترك وهي برمجيات صغيرة تحمل البرامج غير المرغوبة بأجزاء صغيرة في كل مرة يتصل الكمبيوتر بالإنترنت، حتى يتم تثبيت كامل البرنامج.

يسهل إزالة البرمجيات النظامية باستخدام الميزة إضافة أو إزالة البرامج في ويندوز XP، المبينة في الشكل 5-1. فهي تسرد جميع البرامج الموجودة على كمبيوترك وتعطيك الخيار بإلغاء تثبيت كل منها على حدى. فيمكنك أن تستدل على وجود برنامج أدوير أو سبايوير عالي الخطورة بأنه لا يظهر في لائحة البرامج. لكي ترى لائحة البرامج الموجودة على كمبيوترك، انقر على الزر Start ثم اختر Add/Remove. وإذا لم يكن الزر Add/Remove موجوداً في القائمة Start، اختر Control Panel ثم Add or Remove Programs. سوف يظهر برنامج أدوير نظامي في هذه المنطقة ويسمح لك بإزالته.



الشكل (5-1): إضافة أو إزالة البرامج.

تذهب بعض برامج السبايوير إلى أبعد من ذلك بتثبيت نفسها بدون إذنك (على سبيل المثال، تثبت نفسها ولو نقرت "No"، أنا لا أريد هذا البرنامج") أو بدون علمك (تحميل عبر التحول). وبسبب هذه الميزات لبرامج السبايوير والأدوير يصعب البحث عنها وإزالتها.

تدّعي بعض شركات الأدوير أنها تحاول التصرف كمواطن إنترنت صالح. على سبيل المثال، تقول Claria وWhenU أنهما أقسمتا على التخلي عن الخدع القذرة باستخدام التحميل عبر التحول لتثبيت برمجياتها على كمبيوترات المستخدمين. (لكن يناقش بعض الباحثون أنها ما تزال تسبب صعوبة على المستخدمين بالبحث عن برامجها وإزالتها).

لا يزعج بائعو الأدوير الآخرون نفسهم ليظهروا كشركة نظامية ويتابعون بعملهم القذر، حتى مع بعضهم البعض. على سبيل المثال، في عام 2004 اتهمت الشركة Avenue Media الشركة Direct Revenue لإنشاء البرمجيات بالبحث عن أدوير Avenue Media وإزالته وتثبيت الأدوير الخاص بها على كمبيوترات المستخدمين.

إلى جانب التحديات التقنية في منع وإزالة برامج السبايوير والأدوير، توجد قضايا قانونية أيضاً يجب التعامل معها. ومع أنه بعض فئات السبايوير مخالفة للقانون بشكل صريح (مثل مسجلات ضربات المفاتيح)، فإن أدوير تستغل الحالة شبه القانونية. على سبيل المثال، أي برنامج أدوير يخبر المستخدمين عن وظائفه في الاتفاقية EULA هو نظامي على الأغلب. وذلك لأنه يفترض بالمستخدم أن يقرأ ويوافق على الشروط الموجودة في EULA. وقبل أن يبدأ التحميل يجب أن ينقر على زر يقول "أوافق على البنود والشروط

المنصوص عنها في هذا التصريح". إن نقر مثل هذا الزر هو عملية مشابهة لتوقيـــع عقـــد فيزيائي؛ بعد أن تنقر على الزر Yes، فإنك تصبح موافقاً على كل ما تقوله EULA. على كل حال، لا يوجد على الأغلب شخص واحد قد أزعج نفسه وقرأ مستندات EULA، وتعرف شركات الأدوير هذا الأمر. (لمزيد من المعلومات انظر إلى الشريط الجانبي في نهاية هذا الفصل، "قراءة المادة الغامضة").

يوصى بأن تقرأ مستندات EULA لأي موقع تزوره أو برنامج تحمله. فإذا لم يوجـــد لدى البرنامج EULA أو أنه يحاول إخفاء وظيفته بلغة محيرة، فاعتبر ذلك إشارة تحذير لكي لا تحمّل البرنامج.

على كل حال، إحدى القضايا التي تتعرض لنقاش فيما يخص مستندات EULA لبرامج الأدوير هي التعبير عن عملها بشكل وافي. فإذا أشار برنامج أدوير إلى وظائفـــه في الاتفاقيـــة EULA، فهل تعتبر هذه الإشارة كافية؟ ما الأمر إذا تم إخفاء الشرح ضمن اتفـــاق طويـــل وباستخدام لغة محيرة؟

لقد تم اقتراح عدداً من الحلول التشريعية الفيدرالية مؤخراً لمعالجة مشـــكلة الســـبايوير والأدوير، بما في ذلك الإشارة إلى وظائفها. في 1 حزيران 2005، تم تقديم مذكرتين إلى المجلس التمثيلي ومذكرتين إلى مجلس الشيوخ. في المجلس التمثيلي، تم تقديم تشريع يدعى SPY ACT (احمِ نفسك بشكل مؤكد ضد انتهاكات الكمبيوتر، H.R.29) من قبل عضوة مجلس الشيوخ ماري بونو. ويحاول التشريع أن يجعل التصرف غير المقبول، مثل تثبيت برمجيات بدون إذنك، غير قانونياً. وتشترط المذكرة أيضاً على بائعي الأدوير أن يصرّحوا بوضـــوح عـــن وظـــائف البرمجيات، أنواع المعلومات التي يتم جمعها، والهدف من تجميع المعلومات. وتقول المذكرة بأن أدوير يجب أن يمنح المستخدمين القدرة على رفض أو إزالة البرمجيات في أي وقت بدون بذل أي جهد غير ضروري. وتم تقديم مذكرة أخرى إلى المجلس وهي مرسوم المنع I-SPY لعـــام 2005 (H.R.744) من عضو مجلس الشيوخ بوب غادليت في 10 شـــباط 2005. ويركـــز بشكل كبير على أخذ خطوات رادعة وعقوبات قاسية ضد الأشخاص المسيئين. تضيف هذه المذكرة قسم جديد A 1030 إلى النص الإجرامي بعنوان "الاستخدام غير المباشر وغير المشروع للكمبيوترات المحمية" وتحدد ثلاث حالات جنائية محظورة.

وتم تقديم المرسوم SPY BLOCK (S.687) في مجلس الشيوخ من السيناتور كـــونراد بيرنـــز مع عضوي مجلس الشيوخ رون وايدن وباربار بوكر في 20 آذار 2005. ويمنع المرسوم تثبيت البرمجيات على كمبيوتر الغير بدون موافقة ويفرض وجود إجرائيات إزالة تثبيت معقولة لجميع البرمجيات القابلة للتحميل. أما مرسوم حماية المستخدم المعززة ضد السبايوير لعام 2005، المقدم من السيناتور آلن مع عضوي مجلس الشيوخ سميث وإينساين في 11 أيار 2005، فيسمح بحجز أرباح الشركات والأفراد الذين يثبتون السبايوير على الكمبيوترات خلسة. ويـــدعو إلى

اتخاذ عقوبات جنائية ومدنية كبيرة بحق من يستخدم السبايوير. كما يدعو سلطة لجنة التجارة الفيدرالية لمقاضاة عمليات الاقتحام من برامج السبايوير.

تحدد كل من المذكرات الأربعة أن العديد من التقنيات المستخدمة في العمليات الخبيثة والمخادعة يمكن استخدامها أيضاً للأغراض المقبولة والمفيدة. ووفقاً للتشريع، فإن استخدام الأدوير أو سبايوير لا يفترض بالضرورة أن التقنية سيئة أو غير قانونية. بل أن المذكرات تهدف فقط إلى تنظيم الاستخدام السيء للأدوير والسبايوير.

وقد تم المصادقة على H.R.29 وH.R.744 في المجلس في 1 حزيران 2005. ويبقى التصويت على المذكرتين، وأن يتوافق مجلس الشيوخ والمجلس التمثيلي على مذكرة مشتركة يتم المصادقة عليها في كلا المجلسين. وأخيراً يوقع الرئيس على المذكرة فتصبح قانوناً.

يمكنك أن تقرأ المذكرات الأربعة بالذهاب إلى Thomas، صفحة بحث تديرها مكتبة مجلس الشيوخ للبحث عن التشريعات على الوب. اذهب إلى http://thomas.loc.gov واكتب اسم المذكرة أو رقمها في حقل البحث لمجلس الشيوخ 109^{th}.

وبالإضافة إلى النشاطات التشريعية الفيدرالية في هذا العام، فقد تم تقديم أكثر من 40 مذكرة سبايوير إلى الهيئات التشريعية.

كما أن لجنة التجارة الفيدرالية لاحظت مشكلة السبايوير أيضاً. فقد أصدرت اللجنة في آذار 2005 تقريراً بعنوان "مراقبة البرمجيات الموجودة على كمبيوترك: سبايوير، أدوير وبرمجيات أخرى". يصدر التقرير المشاكل المتعلقة بتعريف السبايوير، والمخاطر التي يعرض المستخدمين لها، وكيف يمكن أن تتصرف الحكومة والقيادات الصناعية مع مشكلة السبايوير. لكي تجد نسخة عن التقرير، انظر إلى القسم "موارد مساعدة" في نهاية هذا الفصل.

إن القضايا القانونية عقدت أيضاً جهود بائعي البرمجيات المضادة للسبايوير للتعامل مع الأدوير. ففي عام 2003، رفعت Claria قضية على PC PitStop، مؤسسة برمجيات مضادة للسبايوير، بتهمة الافتراء. فكانت PC PitStop تدعو منتجات Claria بأنها سبايوير، فتعرضت إلى تهمة الافتراء. وفي عام 2005 اشتكى صنّاع برمجيات WeatherBuy الشهيرة عندما ذكرت لائحة منتجات مضادة للسبايوير من مايكروسوفت أنه هناك مكون ملقم إعلاني ضمن WeatherBuy يشكل خطراً على الخصوصية. وقد راجعت مايكروسوفت الشكوى وأزالت التوقيع الذي كشف الملقم الإعلاني.

وقد وجدت بعض المنتجات المضادة للسبايوير نفسها على تعارض مع أعمال أخرى ضمن الشركة نفسها. فقد قدّم Yahoo! على الوب برنامج مضاد للسبايوير مجاني في شريط الأدوات Yahoo!، ولكن عندما تم تشغيل المنتج لأول مرة، طلب من المستخدمين أن يطلبوا

مسحاً للأدوير بالإضافة إلى السبايوير. وذلك لأن القسم Overture من Yahoo! والــذي يقدم لوائح بحث مدفوعة هو شريك لشركة Claria. وفق القصة المنشورة في eWeek[1] في حزيران 2004، فقد قدم Overture لوائح مدفوعة إلى SearchScout، خدمة في كلاريــا تعرض الإعلانات المنبثقة الخلفية. (يتم عرض هذه الإعلانات خلف الصفحة، فتراها بعــد أن تغلق برنامج الاستعراض). لقد كانت SearchScout تؤمن 31 بالمائة من عائدات كلاريا في 2003. وقد غير Yahoo! شريط الأدوات المضاد للسبايوير الذي يقدمه لكي يبحــث عــن الأدوير بالإضافة إلى السبايوير من ذلك الحين.

إحدى الطرق لكي تتجنب شركات البرمجيات المضادة للسبايوير الوقوع في المشاكل هي باعتماد لغة أكثر دبلوماسية. على سبيل المثال، تستخدم البرمجيات المضادة للسبايوير McAfee المصطلح "برامج غير مرغوبة بشكل جاد" بدلاً من "أدوير" أو "سبايوير".

تلتف البرمجيات المضادة للسبايوير من مايكروسوفت على الأمر بالإشارة إلى أي شــيء "كبرمجيات غير مرغوبة أبداً". (إذا أخذت اختصار من هذه الكلمات فسوف يكــون PUS والذي يعني القيح. لا أعرف إذا كان القائمون على ذلك في مايكروسوفت قد اختاروه عمداً، لكنه يستحضر بشكل عام شعور الأشخاص الذين يضطرون للعمل مع هذا الشيء. كما أنــه أقصر من مصطلحي، والذي يمكن أخذ اختصار منه: Bad والذي يعني سيء، برمجيات مزعجة يحتاج كل شخص إلى إزالتها على وجه السرعة).

هل تريد كعكة؟

تبرز مع الكعكات مشكلة أخرى في التعامل مع البرامج غــير المرغوبــة وتصــنيفها. الكعكات هي ملفات نصية يضعها ملقم الوب على كمبيوترك عندما تزور موقع وب. تحتوي الكعكات على معلومات عنك كأفضلياتك ومعلومات تسجيل الدخول. وفي كل مرة تعــود إلى موقع وب، يتم إرسال الكعكة المناسبة من كمبيوترك إلى موقع الوب من أجل تخصــيص زيارتك. على سبيل المثال، إذا كنت زبوناً لموقع تجارة إلكترونية، فقد يحفــظ هــذا الموقــع معلومات عنك في كعكة على كمبيوترك، مثل سجل التسوق، أفضليات الشــراء وهكــذا. فالكعكات تسهل عمل التجارة الإلكترونية وهي غير خطرة بشكل عام.

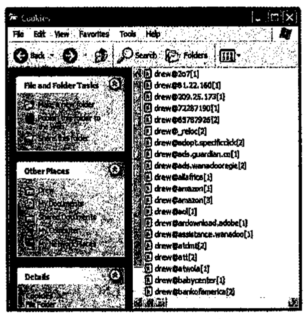
على كل حال، توجد فئة أخرى من الكعكات، تدعى كعكــات التعقــب، تســجّل معلومات عن مواقع الوب الأخرى التي زرتها وتشارك هذه المعلومات مع المواقــع الأخــرى. وتجمع شبكات الإعلان هذه المعلومات لإجراء بحث السوق ومساعدتها على تخديم الإعلانات

(1) "يؤدي Yahoo لعبته المفضلة مع بعض الأدوير"، الكاتب مات هيكس، تم نشره في 1 حزيــران 2004 في eWeek (www.eweek.com).

الموجهة إلى كمبيوترك. يجب أن تكشف البرمجيات المضادة للسبايوير الجيدة كعكات التعقب وتعطيك الخيار بحذفها.

يمكنك أن ترى الكعكات على كمبيوترك بالذهاب إلى My Computer ونقر محـرك القرص (:C)، ثم Documents and Settings، ثم اسم المستخدم وبعدئذ المجلـد Cookies. على كل حال، لن يخبرك مجرد النظر إلى الكعكات الشيء الكثير عما إذا كانت كعكة قياسية أو كعكة تعقب. تتألف معظم الكعكات من عدد كبير من الأرقام التي يفهمها ملقم الـوب، ولكنها غير ذات معنى للإنسان. وبالنظر إلى لائحة الكعكات يمكنك أن ترى أي مواقع الوب يحفظ الكعكات على محرك القرص لديك. فيمكنك أن تحذفها بتمييز الملف المحدد ونقر الـزر Delete لحذف الملف على الجانب الأيسر من النافذة، كما هو مبين في الشكل 5-2.

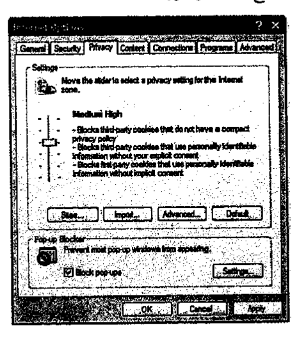
يمكنك أن تتحكم أيضاً بطريقة إعداد مواقع الوب للكعكات على كمبيوترك وذلـك بتعديل إعدادات الخصوصية في برنامج استعراض الـوب. وإذا كنـت تسـتخدم إنترنـت إكسبلورر، افتح برنامج الاستعراض وحدد Tools، Internet Options، Privacy. يعـدل



الشكل (5-2): حذف الكعكات.

شريط الزالقة إعداد الخصوصية فيحدد نوع الكعكات التي يقبلها برنامج الاسـتعراض، كما هو مبين في الشكل 5-3. تتراوح الخيارات من قبول جميع الكعكات إلى حجـز جميـع الكعكات، مع جميع الدرجات بينهما. الإعداد الافتراضي في مايكروسـوفت هـو الأعلـى المتوسط Medium High، ويعني أن برنامج الاستعراض سوف يحجز أي كعكة تحـاول أن تستخدم المعلومات الشخصية بدون موافقة صريحة بذلك.

تذكر أنه ليس جميع الكعكات مؤذية، على سبيل المثال، إذا حذفت الكعكات من مواقع التجارة الإلكترونية التي تستخدمها عادةً، قد يتم إزالة التخصيص الذي تستمتع به. وإعـداد حماية الكعكات إلى مستوى مرتفع جداً قد يمنعك من دخول بعض المواقـع. علـى سـبيل المثال، حسابي البريدي على Yahoo! Web لا يعمل مع الإعـداد Block All Cookies أو High Security في إنترنت إكسبلورر. يتم نقاش إعداد الكعكة بمزيد من التفصيل في الفصل السابع، "تأمين ويندوز".



الشكل (3-5): خيارات إعداد الكعكات في IE.

كائنات المشاركة المحلية (LSO) هي مثال آخر عن كائنات التعقب، مثـل كعكـات برنامج ماكرو ميديا فلاش. يمكن أن يستخدم موقع الوب LSO لحفـظ المعلومـات علـى كمبيوترك كعلامة مرتفعة في لعبة أو معلومات قمت بإدخالها (مثل اسمك وعمرك). ولكـن ليس كما مع الكعكات، لا يمكنك أن تلغي تأهيـل LSO باسـتخدام إعـدادات برنـامج الاستعراض العادية.

3-5 كيف تصيب برامج السبايوير، الأدوير وأحصنة طروادة كمبيوترك

يمكن أن تصل السبايوير، الأدوير وأحصنة طروادة إلى كمبيوترك بعدد من الطرق بما في ذلك من برنامج استعراض الوب، عن طريق البريد الإلكتروني أو ضمن حزمة البرمجيات الـتي تحمّلها. وبمعرفة كيف تصل هذه البرمجيات إلى كمبيوترك، تحصل على فكرة أفضل عن طريقة إبعادها.

من برنامج الاستعراض

أحد الأسباب أن انتشار استعراض الوب هو وسيلة شائعة لنقل السبايوير والأدوير هو أكتيف إكس، وهي تقنية من مايكروسوفت صممت لتأهيل الكائنات المتضمنة والتفاعلية، وملفات الوسائط المتعددة على صفحات الوب. تعمل أكتيف إكس على جعل صفحة الوب أكثر تفاعلية باستخدام التحريك أو بفتح تطبيقات أخرى في برنامج الاستعراض (مثل مايكروسوفت وورد أو أدوبي).

تستطيع التقنية أكتيف إكس، إلى جانب بث الحياة في صفحات الوب، أن تنفذ برامج على كمبيوترك عبر برنامج استعراض الوب إنترنت إكسبلورر، وتدعى تحكمات أكتيف إكس. تتفاعل هذه التحكمات مع نظام التشغيل مثل البرمجيات القابلة للتنفيذ الأخرى. وتأتي البرامج أكتيف إكس مع تواقيع رقمية من كاتب البرنامج (أي الشركة التي أنشأت البرنامج، وليس مهندس البرمجيات الفعلي). فكّر بالتوقيع الرقمي كتوقيع الشخص على الورق. يستطيع برنامج الاستعراض أن ينظر إلى التوقيع الرقمي ويرى فيما إذا كان التوقيع أصلي فتعرف بالتأكيد من الذي وقّع البرنامج. يوجد لديك خياران: إما أن تقبل بالبرنامج وتدعه يفعل ما يحلو له على كمبيوترك أو ترفضه. يعتمد أمن أكتيف إكس عليك في اتخاذ القرارات الصحيحة حول البرامج التي تقبلها. فبعض تحكمات أكتيف إكس غير مؤذية وتحسن من تجربة الاستعراض، لكن مبرمجو المالوير ينشئون أيضاً تحكمات أكتيف إكس لتثبيت البرامج غير المرغوبة على كمبيوترك. وإذا قبلت برنامجاً خبيثاً، فسوف تقع في ورطة كبيرة.

يمكنك أن تضبط برنامج الاستعراض إنترنت إكسبلورر بحيث يتم توجيهك عند محاولة تحميل تحكم أكتيف إكس إلى كمبيوترك. ولكي تعرف الطريقة، انظر إلى القسم "ضبط إعدادات برنامج الاستعراض".

يمكن أن يستغل مبرمجو السبايوير والمالوير أيضاً نقاط الخلل في برامج الاستعراض (بما في ذلك برامج الاستعراض البديلة مثل Mozilla Firefox). فكل منتج برمجي يملك نقاط خلل ويكتشفها الباحثون. بعض هؤلاء الباحثين هم محترفون أمنيون؛ وبعضهم الآخر مهاجمون خبيثون يستخدمون الاكتشاف الجديد لمهاجمة البرمجيات التي تحتوي على خلل. وبما أن إنترنت إكسبلورر هو برنامج الاستعراض الأكثر استخداماً في العالم، فهو هدف شائع للمهاجمين. على سبيل المثال، في حزيران 2004 ظهر حصان طروادة يدعى Download.ject. وبالاستفادة من نقاط الخلل الموجودة في IE وIIS (ملقم معلومات الإنترنت، وهو برمجيات ملقم الوب لويندوز)، قام حصان طروادة بتثبيت نفسه على كمبيوترات المستخدمين بمجرد أن يزوروا موقعاً يعمل في ملقم وب مصاب. إن Download.ject هو مثال عن التحميل بالتحول على

الوب. أما عمليات الهجوم التي تستغل نقاط الخلل في البرمجيات فيتم التعامل معها بأفضل شكل باستخدام الحلول البرمجية التي تدعى الرقع، والتي ينشئها ويوزعها بائع البرمجيات. على سبيل المثال، في كل ثاني ثلاثاء من كل شهر، تصدر مايكروسوفت الرقع الأحدث لبرمجياتها. لكي تحمل الرقع، اذهب إلى الموقع http://windowsupdate.microsoft.com.

من البرمجيات الأخرى

إن الطريقة الأكثر شيوعاً لنشر أدوير هي بوضعه مع برامج أخرى، مثل برمجيات مشاركة الملفات أو أدوات التسلية. وفي بعض الأحيان يخبرك مزود البرمجيات التي تريدها بأنه يتم تثبيت الأدوير.وأحياناً أخرى لا يخبرك. وفي العديد من الحالات، لا تعمل البرمجيات التي تريدها، مثل برنامج مشاركة الملفات، إذا ألغيت تأهيل الأدوير الذي يأتي معها. (انظر إلى الشريط الجانبي لاحقاً "قراءة المادة الغامضة".

من البريد الإلكتروني

يمكن أن تصل برامج السبايوير وأحصنة طروادة إلى كمبيوترك كارتباطات مع البريد الإلكتروني. على سبيل المثال، العديد من عمليات هجوم التصيد، والتي يستخدم فيها المجرم خدعة البريد الإلكتروني لكي يخدعك ويكشف كلمات المرور، أرقام الضمان الاجتماعي، ومعلومات حساسة أخرى، تضم أيضاً برامج مالوير مثل مسجلات ضربات المفاتيح.

من الهندسة الاجتماعية

كما تم نقاشه في الفصل الثاني، "منع سرقة الهوية"، الهندسة الاجتماعية هي طريقة مهذبة لوصف الكذب. لا يتورع مبرمجو السبايوير والأدوير عن الكذب لكي يحملوك على تثبيت برمجياتهم. المثال الأكثر انتشاراً من الهندسة الاجتماعية هو الإعلان عن برنامج أو ملحق بريد إلكتروني على غير حقيقته. مثل الدودة Naked Wife التي ظهرت في 2001. تنتشر هذه الدودة عبر البريد الإلكتروني وتضم ملفاً ملحقاً يتبين أنه فيلم فلاش مزعج. ولكن بالفعل فإن الملف المرتبط هو حصان طروادة يتم تثبيته على كمبيوترك، ويرسل نفسه بالبريد الإلكتروني إلى جميع العناوين الموجودة في دليل عناوينك، ثم يبدأ بحذف الملفات.

4-5 كيف تحمي نفسك من سبايوير، أدوير وأحصنة طروادة

يمكنك أن تحمي كمبيوترك من الإصابة بسبايوير، أدوير وأحصنة طروادة بطرق متعددة. يشرح هذا القسم عدة طرق.

استخدام البرمجيات المضادة للسبايوير والمضادة للفيروسات

إن الطريقة الأفضل لكي تحمي نفسك من السبايوير وأحصنة طروادة هي باستخدام البرمجيات المضادة للسبايوير والبرمجيات المضادة للفيروسات. يمكن أن يمنع كلا النوعين من البرمجيات تثبيت برامج سبايوير وأحصنة طروادة المعروفة على كمبيوترك، ويمكن أن يمنع تثبيت برامج مالوير غير المعروفة أيضاً.

يقدم العديد من باعة البرمجيات المضادة للفيروسات حماية من السبايوير والأدوير كجزء من مجموعة أكبر تضم البرمجيات المضادة للفيروسات وجدار نار. إن هذه المجموعات هي خيار رائع لأن إدارتها أسهل من إدارة المنتجات المستقلة. وبالإضافة إلى ذلك، تريحك من مشكلة أن المنتج A يسبب انخفاض في أداء المنتج B (أو أن المنتجين A وB يسببان انخفاض أداء كمبيوترك).

قد تظل بحاجة إلى حماية إضافية من البرمجيات المضادة للسبايوير المخصصة. لماذا؟ السبب الأبسط هو استراتيجية الدفاع بالعمق (تدعى أيضاً طريقة الحزام والعلاّقات)؛ وقد يلتقط أحد المنتجات السبايوير أو الأدوير التي تفلت من المنتجات الأخرى.

فإذاً لماذا لا تستخدم منتجين مختلفين من البرمجيات المضادة للفيروسات أيضاً؟ بالفعل، تستخدم العديد من الشركات هذه الاستراتيجية: يتم تحميل ملقمات البريد الإلكتروني بالبرمجيات المضادة للفيروسات من الشركة AV رقم 1، بينما تحصل الكمبيوترات المكتبية على البرمجيات المضادة للفيروسات من الشركة AV رقم 2. على كل حال، لا يحتاج المستخدمون فعلياً إلى منتجين مختلفين من البرمجيات المضادة للفيروسات. بشكل عام، جميع باعة البرمجيات المضادة للفيروسات ينجزون عملاً جيداً كغيرهم.

ولكن هذه الحالة غير صحيحة بالضرورة بالنسبة للسبايوير والأدوير. فشركات البرمجيات الأمنية ما تزال تعارك لكي تعرّف بالضبط ما هو السبايوير والأدوير. وكل شركة تضع مجموعة تعاريف خاصة بها، وبالتالي فإن كل شركة تعرّف وتتعامل مع السبايوير والأدوير بطريقة مختلفة قليلاً. وفوق ذلك، أثبت مبرمجو السبايوير والأدوير ذكاءهم وإبداعهم، وهم يجدون بشكل دائم طرق جديدة للوصول إلى كمبيوترك. وتظهر برامج سبايوير وأدوير جديدة بمعدل لا يصدق، كما قد تحصل إحدى الشركات على التواقيع قبل الأخرى أو تنشر أداة إزالة بشكل أسرع من الأخرى. وبالنتيجة قد تتفوق الحماية المضادة للسبايوير من الشركة A في بعض النواحي على مثيلاتها وقد تخفق في نواحٍ أخرى، والعكس بالعكس بالنسبة إلى الشركة B.

يمكنك أن تشتري البرمجيات المستقلة المضادة للسبايوير من عدد من الباعة، وتحصل على عدد من الخيارات المجانية الجيدة. لذلك حتى لو كانت البرمجيات AV الموجودة لديك تبحث

عن السبايوير، فقد يكون من الأفضل أن تختبر كمبيوترك باستخدام أداة أخرى مضادة للسبايوير. يذكر الجدولان 5-3 و5-4 البرمجيات الرئيسية المضادة للسبايوير، بنوعيها المدفوعة والمجانية.

وبالتالي إذا استخدمت برنامجين منفصلين مضادين للسبايوير، فلا تُفاجأ إذا بدؤوا بالتسبب بالمشاكل. إذا كانت الحال كذلك، يجب أن تقرر ما هو البرنامج المفضل لديك وتتخلى عن الآخر.

وتضم الأسماء الكبيرة في سوق البرمجيات المضادة للسبايوير Aluria Software التي تقدم Spyware Eliminator؛ Sunbelt Software، التي تقدم CounterSpy؛ Webroot Software، التي تقدم Spy Sweeper؛ Lavasoft، التي تقدم Ad-Aware؛ Tenebril، التي تقدم Spy Catcher؛ وComputer Associates التي تبيع eTrust PestPatrol. كما يبيع أيضاً باعة البرمجيات المضادة للفيروسات الأدوات المضادة للسبايوير، ويقدم البائعون الصغار أيضاً منتجات مقبولة. يسرد الجدول 5-3 الباعة. وفي منتصف 2005 كانت الأسعار تتراوح من 19.95$ إلى 29.95$ للبرمجيات المستقلة المضادة للسبايوير، و49.95$ إلى 69.95$ للمجموعات الأمنية التي تضم البرمجيات المضادة للسبايوير، البرمجيات المضادة للفيروسات، جدار نار ومنتجات أمنية أخرى. لاحظ أن العروض الخاصة والمساومات قد تؤثر على السعر النهائي.

الجدول (5-3):

المنتجات التجارية المضادة للسبايوير		
المنتج	البائع	موقع الوب
Active Scan Pro	Panda Software	www.pandasoftware.com
Ad-Aware SE Plus	Lavasoft	www.lavasoft.com
counterSPY	Sunbelt software	www.sunbeltsoftware.com
eTrust PestPatrol	Computer Associates	www.ca.com
F-Secure Anti-Spyware	F-Secure	www.f-secure.com
McAfee Antispyware	Mcafee	www.mcafee.com
PC-cillin	Trend Micro	www.trendmicro.com
SpyCatcher	Tenebril	www.tenebril.com
SpySweeper	Webroot Software	www.webroot.com
Spyware Eliminator	Aluria software	www.aluriasoftware.com
Symantec Norton Internet Security Spyware Edition	Symantec	www.symantec.com

عندما تختار منتجاً ابحث عن نظام يسمح لك بإجراء عمليات مسح دورية وإجراء الكشف بالزمن الحقيقي لبرامج السبايوير الخطيرة. ابحث عن المنتجات التي يمكنها أن تكشف وتزيل السبايوير وتحجر البرامج المشبوهة. (تقوم وظيفة الحجر بمنع تشغيل البرنامج لكنها لا تزيله). وتسألك البرامج المضادة للسبايوير، مثل جدران النار والبرامج AV، عما ستفعله مع البرامج المكتشفة. في بعض الأحيان يكون القرار سهلاً، وفي أحيان أخرى قد لا تكون أكيداً. تقدم البرامج المضادة للسبايوير غالباً معلومات عن البرامج المكتشفة، ولكن قد تكون هذه المعلومات تقنية فلا يمكنها مساعدتك. لذلك ابحث عن منتج يقدم المعلومات المهمة بطريقة ذكية تساعدك على اتخاذ القرار.

يجب أن تحافظ أيضاً على تحديث البرمجيات محدثة بشكل دوري، لذلك ابحث عن واجهة تسمح بإجراء عمليات التحديث. واستفد من الفترات التجريبية المجانية لكي تختار الواجهة الأفضل.

لكي تحصل على المساعدة باختيار المنتج الذي سوف تستخدمه، يمكنك قراءة المواضيع في PC Magazine (www.pcmagazine.com)، PC World (www.pcworld.com)، وCNET (www.cnet.com) والتي تراجع وتقيّم المنتجات الأمنية بشكل دوري. ويمكنك أيضاً أن تنظر إلى المنتديات على الوب وتقرأ التوصيات والمقالات. توجد منتديات جيدة في CastleCops (www.castlecops.com) وSpywareInfo (www.spywareinfo.com).

احذر من الانتهازيين

لقد ظهرت البرمجيات المضادة للفيروسات منذ سنوات. وفي هذا الوقت تم القضاء على المنتجات الضعيفة، وطورت الشركات المشهورة منتجات مستقرة تعمل وفق المواصفات التي يتم التصريح عنها. ما تزال سوق البرمجيات المضادة للسبايوير في بداياتها، ويجب على قوة السوق التي تبعد الأعمال غير الجيدة أو الضعيفة أن تبذل قصارى جهدها. لقد ظهرت في السوق العديد من المنتجات، وهي لا تعمل بشكل جيد جداً. وتحاول بعض المنتجات التسبب بحيرة المستخدمين بأخذ أسماء مشابهة أو تسجيل مواقع الوب المشابهة للبرمجيات المضادة للسبايوير المشهورة. على سبيل المثال، يتم استخدام اسم أداة شائعة ضد قرصنة برامج الاستعراض HijackThis من المقلدين أو مبرمجي المالوير لكي يجذبوا المستخدمين إلى مواقعهم. تتوفر الأداة الحقيقة HijackThis في www.merijn.org/downloads.html.

بالإضافة إلى ذلك، فإن الفرص المقدمة من القطاع التقني الجديد تجذب المستخدمين بالخدع البغيضة (أو غير القانونية) لإقناعهم بشراء برمجياتها. على سبيل المثال، في أيار 2005 قدمت FTC شكوى ضد منتج يدعى Spyware Assassin. فقد ادعت FTC بأن Spyware Assassin قد قدم عمليات مسح مجانية مضللة ادعى فيها بأنه يكشف السبايوير

على كمبيوترات المستخدمين، حتى عند عدم وجود سبايوير. وقد مضـت الخدعـة قـدماً وذكرت أسماء ومواقع ملفات السبايوير على كمبيوترات نظيفة تماماً. ثم قـدم Spyware Assassin برمجيات مضادة للسبايوير (بكلفة 29.95$)، وتدعي FTC بأنها لا تعمل جيداً.

إذا لم تذهب إلى موقع محدد وتطلب عملية المسح، احذر من النوافذ المنبثقة وغير المطلوبة التي تحثك على نقر زر أو إجراء مسح بشكل فوري – أو التي تدعي بأنها كشفت سـبايوير على كمبيوترك بدون أن تطلب إجراء عملية مسح. يجب أن تحذر من اسـتراتيجيات البيـع المشابهة، كما تحذر منها في حياتك العملية.

إن الباعة المذكورين في اللائحة ذوي سمعة جيدة، ويجب أن تشعر بارتياح للعمل مـع منتجاتهم. إذا لم يكن البائع مذكوراً في اللائحة، لا يعني ذلك أن منتجه سيء أو مضلل. أي إذا كنت تتعامل مع شركة مغمورة، فكن حذراً. على سبيل المثال، تقدم الشركات المشهورة سياسة الخصوصية وEULA على موقع الوب. وإحدى الطرق لكي تتحرى عن شركة معينة هو أن تبحث عن اسمها في محرك بحث وترى النتائج. يمكنك أن تدخل أيضاً إلى منتدى مضاد للسبايوير لتأخذ فكرة عن سمعة الشركة أو لكي تعرف مواقف الآخرين من الشركة إيجابية أم سلبية.

البرمجيات المجانية المضادة للسبايوير

إن الشيء الأفضل في البرمجيات المضادة للسبايوير المجانية كونها مجانية! فإذا لم ترغـب بالدفع من أجل البرمجيات المضادة للسبايوير، فإن هذه الخيارات المجانية مناسبة تماماً. ويمكـن استخدامها أيضاً كنسخة احتياطية للبرمجيات المدفوعة لكي تضمن أن نظامك نظيـف قـدر الإمكان (أو لكي تدقق أن البرمجيات المدفوعة تقوم بعملها على أكمل وجه). لاحظ أنـه إذا كنت تستخدم عدة أدوات مضادة للسبايوير فقد يذكر أحدها الأخرى بأنها سبايوير. علـى سبيل المثـال، العديـد مـن البرمجيـات المضـادة للفيروسـات تكتشـف أن Spybot Search&Destroy، برنامج مجاني مضاد للسبايوير، بأنه سبايوير.

إن الجانب السيء في البرمجيات المجانية هو أنه قد ينقصها بعض المزايا، مثل الدعم التقني. بالإضافة إلى أن بعض البرمجيات المجانية المضادة للسبايوير يكتبها شخص واحـد أو مجموعـة صغيرة من المتطوعين، ويعني ذلك أنهم قد يكونوا أبطأ في تقديم التواقيع الجديدة، المزايا الجديدة والحلول البرمجية من المنتجات التجارية. قد تحتاج أيضاً إلى تحميل ملفات التحديث الجديـدة يدوياً، في حين أن المنتجات التجارية تقدم عمليات التحديث التلقائية.

يعتبر Lavasoft's وSpybot Search&Destroy البرنامجان الأكثر انتشاراً مـن بـين البرمجيات المجانية المضادة للسبايوير. كما أن Lavasoft تبيع إصدار تجاري من Ad-Aware، لكن Spybot مجاني (على الرغم أنه يمكنك التبرع إلى مبرمجه إذا وجدت البرنـامج مفيـداً).

وكلا البرنامجين Lavasoft وSpybot Search&Destroy يقدمان منتديات يمكنك طرح الأسئلة فيها والاطلاع على معلومات جديدة عن البرمجيات.

أصدرت مايكروسوفت في كانون الثاني 2005 أداة مجانية مضادة للسبايوير تدعى، Microsoft AntiSpyware. وقد تم الحصول على البرنامج الداخلي من شركة البرمجيات GIANT Software. وتقدم هذه البرمجيات إمكانية المسح والحجز. يمكنك أن تشترك أيضاً في مجتمع SpyNet، منتدى لتجميع المعلومات عن البرمجيات غير المرغوبة وإصدار تقارير بها.

هناك أداة مجانية أخرى معروفة جيداً هي الماسح المضاد للسبام المبيّت في شريط أدوات Yahoo!. ولديها مزايا أخرى مثل الحاجز المنبثق وارتباطات إلى مواقع ياهو الأخرى. إذا حمّلت شريط الأدوات يمكنك الوصول إلى المنتدى المضاد للسبايوير حيث يمكنك وضع رسائل والحصول على معلومات حول تهديدات سبايوير الجديدة. لاحظ أن الماسح المضاد للسبايوير في شريط الأدوات Yahoo! يعتمد على البرمجيات eTrust PestPatrol للشركة Computer Associates.

أخيراً، يمكنك أن تحمل أداتين مجانيتين مفيدتين – HijackThis وCWShredder. تقدم HijackThis سجل للمسجل Registry، يمكنك أن تستخدمه لكشف البرامج غير المرغوبة مثل قراصنة برامج الاستعراض. أما CWShredder فهي أداة لإزالة أدوير CoolWebSearch، وهي عائلة من اكثر برامج المالوير عناداً وخبثاً على الإنترنت. وقد اشترت الشركة TrendMicro الشركة InterMute التي تقدم CWShredder من أجل التحميل المجاني. في الوقت الذي كتبت فيه هذا الفصل، كان CWShredder ما يزال متوفراً في www.intermute.com/products/cwshredder.html. على كل حال، قد يتغير ذلك، وقد تحتاج إلى البحث في www.trendmicro.com عن البرمجيات أو تحملها من موقع الوب Merijn Bellekom، الذي أنشأ CWShredder (أو HijackThis). يذكر الجدول 5-4 هذا الموقع ومواقع البرمجيات المجانية الأخرى.

ما الذي يمكن أن تقوم به البرمجيات المضادة للسبايوير

تمسح المنتجات المضادة للسبايوير محرك القرص الصلب من أجل البرمجيات غير المرغوبة. وعندما تكشف هذه البرمجيات، تسألك فيما إذا كنت تريد حذفها، حجرها أو تركها على حالها. (يتم حجر برامج السبايوير بتركها على كمبيوترك ومنعها من العمل). تؤمن العديد من المنتجات عملية مراقبة وقائية لتضمن أن البرامج غير المرغوبة غير مثبتة على كمبيوترك في المقام الأول. على سبيل المثال، يتضمن Microsoft AntiSpyware مكونات تراقب تطبيقاتك وإعدادات نظام الكمبيوتر في الزمن الحقيقي. وتنبهك إذا جرت محاولات لتغيير التطبيقات أو الإعدادات. وتراقب البرامج على كمبيوترك التي تحاول الوصول إلى الإنترنت.

الجدول (5-4):

البرمجيات المجانية المضادة للسبايوير		
المنتج	البائع	موقع الوب
Ad-Aware SE Personal	Lavasoft	www.lavasoft.com
HijackThis وCWShredder*	Merijn/InterMute	www.merijn.org/downloads.html (من أجل HijackThis وCWShredder) http://www.intermute.com/products/cwshredder.html (من أجل CWShredder)
Microsoft AntiSpyware	Microsoft	www.microsoft.com
Spybot Search&Destroy	Safer-Networking	www.safer-networking.org
Yahoo! Toolbar مع Anti-Spy	Yahoo!	http://toolbar.yahoo.com/ie

- *HijackThis وCWShreadder ليسا حلول مضادة للسبايوير كاملة. HijackThis هو أداة لإزالة برامج قرصنة برنامج الاستعراض يدوياً. وCWShredder هو أداة إزالة للبرنامج CoolWebSearch فقط، والذي أصدر عائلة كاملة من إصدارات السبايوير. لاحظ أيضاً أن مواقع الوب Merijn، Lavasoft وSpybot تقع في بعض الأحيان ضحية لهجوم رفض الخدمة أو لمحاولات فصلها عن الوب. إذا وجدت أن هذه المواقع غير متاحة، حاول الوصول إليها لاحقاً.*

تستخدم البرمجيات المضادة للسبايوير، مثل البرمجيات AV التي تم نقاشـها في الفصـل الرابع، التواقيع لكشف برامج المالوير على كمبيوترك. وكما تتذكر فإن التوقيع مثل البصـمة لجزء محدد من المالوير. تمسح البرمجيات المضادة للسبايوير الملفات، المسجلات، والبرامج علـى محرك القرص الصلب، وتبحث عن هذه البصمات. لكي تعمل البرمجيات المضادة للسـبايوير بفعاليتها القصوى، يجب أن تحدّث بشكل مستمر قاعدة بيانات التواقيع. يجب أن تمسح أيضاً كمبيوترك بشكل دوري لكي تضمن عدم وصول سبايوير جديد إلى كمبيوترك. إذا أمكـن الأمر، امسح كمبيوترك مرة على الأقل في الأسبوع.

قد ترغب أيضاً بأن تمسح كمبيوترك قبل إجراء معاملة مهمة على الوب، مثل معاملـة مصرفية على الوب أو أي معاملات مالية أخرى. كما تم نقاشه في الفصل الثاني، يحاول مجرمو سرقة الهوية أن يزرعوا السبايوير أو أحصنة طروادة على كمبيوترك لسرقة معلومات تسـجيل الدخول وكلمات المرور. أو حق التسلل إلى الجلسات المفتوحة لعقد صـفقات لصـالحهم. يمكنك أن تشعر بمزيد من الثقة في المعاملات على الوب عندما تجري المسح قبل إجراء المعاملة.

كما أن بعض الشركات بدأت بتقديم عمليات مسح مجانية عن برامج المالوير لزبائنها قبل أن يبدؤوا بتنفيذ معاملات مهمة.

ما الذي لا يمكن أن تقوم به البرمجيات المضادة للسبايوير

بما أن البرمجيات المضادة للسبايوير تعتمد على التواقيع، فإنها بحاجة إلى نسخة من كل برنامج سبايوير معروف لتنشئ البصمة. ومثل البرمجيات AV، فإن البرمجيات المضادة للسبايوير لا تضمن أن تمنع برامج السبايوير الجديدة من إصابة كمبيوترك.

لا تقدم البرمجيات المضادة للسبايوير حماية كاملة من جميع أصناف المالوير. وفي حين أن المنتجات AV والبرمجيات المضادة للسبايوير أخذت بالتداخل فيما بينها، فإن البرمجيات المضادة للسبايوير لا تقدم حماية كافية بحد ذاتها من الفيروسات، الديدان وأحصنة طروادة. بالإضافة إلى ذلك، فإن المنتجات المضادة للسبايوير قد لا تمسح بريدك الإلكتروني والذي أصبح وسيلة شائعة للإصابة بالسبايوير. يجب أن تشغل البرمجيات AV والبرمجيات المضادة للسبايوير لتحصل على الحماية الكاملة.

اشتبه بالبرمجيات المجانية

تعج الإنترنت بالبرمجيات المجانية، بما في ذلك الألعاب، برامج مشاركة الملفات، شاشات التوقف، وهكذا. بعض هذه البرامج غير مؤذ البتة، ولكن بعضها الآخر ليس كذلك. تقدم الشركات غالباً البرمجيات المجانية التي تتضمن برامج الأدوير أو السبايوير. يجب أن تشتبه بعروض البرمجيات المجانية. فإذا لم تتضمن البرمجيات الاتفاقية EULA، بيان خصوصية، وتعليمات واضحة عن طريقة إزالة البرمجيات لاحقاً، يجب أن تتجنب تحميلها.

اقرأ الاتفاقية EULA

إن اتفاقية تصريح المستخدم (EULA) هي عقد بينك وبين بائع البرمجيات. عندما تحمّل وتثبت البرمجيات، يتم عرض شاشة تبين الاتفاقية EULA. ولا تسمح البرمجيات بمتابعة التثبيت حتى تنقر زر للإعلام بأنك قرأت وفهمت مصطلحات الاتفاقية. ينقر معظم الناس الزر بدون قراءة التصريح.

إنه خطأ، خصوصاً مع البرمجيات المجانية، لأنها غالباً ما تضم أدوير أو برامج غير مرغوبة أخرى. فالشركات النظامية التي تقدم البرمجيات المجانية تخبرك عن وجود الأدوير في أحد أجزاء الاتفاقية EULA (ربما في الجزء الأخير) وتعطيك الخيار برفض كامل الحزمة. إذا فهمت أن قبول البرمجيات المجانية يعني قبول الأدوير أيضاً، يجب أن تتابع في عملية التحميل.

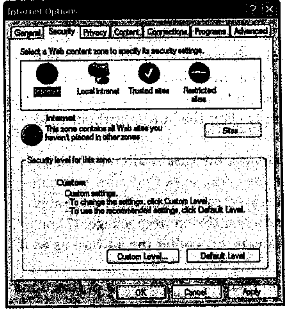
إذا قرأت EULA و لم تجد ذكراً للبرامج أو الوظائف التي تراقب استخدام كمبيوترك،

ثم اكتشفت لاحقاً أن البرمجيات لا تتضمن البرامج غير المرغوبة، يمكنك إرسال تقرير عن مزود البرمجيات إلى FTC. فاللجنة FTC تتخذ إجراءات ضد الشركات التي تنخرط في الممارسات المضللة. انظر إلى القسم "موارد مساعدة" في نهاية هذا الفصل لمزيد من المعلومات حول إرسال الشكاوى.

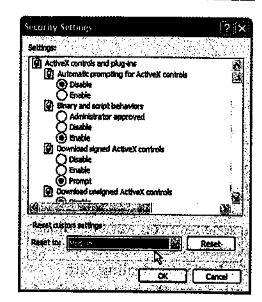
اضبط إعدادات برنامج الاستعراض

يمكنك أن تضبط إعدادات برنامج الاستعراض IE بحيث يحذرك عندما يتم محاولة تحميل تحكم أكتيف إكس فيترك لك القرار بقبول أو رفض عملية التحميل. لكي تـدقق الإعـداد، افتح IE وحدد Tools ثم Internet Options، ثم انقر علامة التبويـب Security. فتـرى أربع مناطق لضبط الإعدادات الأمنيـة: Internet الإنترنـت، Local intranet الإنترنـت المحلية، Trusted sites المواقع الموثوقة وRestricted sites المواقع المحظورة، كما هو مبين في الشكل 5-4.

لكي تغير إعدادات كل منطقة، انقر رمز المنطقة التي تريـد تعديلـها، ثم انقـر الـزر Custom Level. فيتم فتح إطار جديد يدعى Security Settings، كمـا هـو مـبين في الشكل 5-5. يمكنك إعداد قواعد منفردة للتعامل مع تحكمات أكتيف إكس أو تختار ببساطة الإعداد Medium قرب أسفل مربع الحوار. طالما أعددت أمن IE على Medium، تحصـل على رسالة تحذيرية؛ ويسمح أي إعداد آخر بتحميل لتحكمات أكتيف إكس بدون إعـلام. (كما ذكرنا، يتم تغطية أمن برنامج الاستعراض بمزيد من التفصيل في الفصل السابع).



الشكل (5-4): خيارات أمن الإنترنت.



الشكل (5-5): مربع حوار الإعدادات الأمنية.

لسوء الحظ، حتى عندما ينبثق مربع حوار لينبهك عن التحميل، فإن النقر عليه لا يساعد كثيراً. فبعض مبرمجي المالوير يعدلون مربع الحوار بحيث يتم المتابعة في تحميل البرمجيات بغض النظر عن نقر الزر No أو أي زر آخر. ويحاول المهاجمون أيضاً تزوير الرسائل المنبثقة لكي تبدو كرسائل من كمبيوتر ويندوز عن تحكم أكتيف إكس أو يجعلوها تبدو كأنها صادرة عن موقع الوب الذي تزوره. تكون هذه الرسائل عادةً تنبيهية وتحثك على اتخاذ خطوات فورية، مثل نقر الزر Yes لبدء عملية مسح أو تحميل برنامج لإصلاح "المشكلة". يجب أن تتجاهل هذه الرسائل.

لكي تغلق مربعات الحوار والأطر المنبثقة بدون نقر الزر No أو Cancel أو الرمز X في الزاوية العليا اليمنى، يمكنك أن تضغط F4+Alt. فيغلق ذلك جميع الأطر ضمن برنامج الاستعراض بدون أن يسمح بتنفيذ أي عملية تحميل.

استخدام برنامج استعراض بديل

هناك خيار آخر لمساعدتك بمنع تحميل السبايوير إلى كمبيوترك وهو باستخدام برنامج استعراض غير إنترنت إكسبلورر. على سبيل المثال، لا يستخدم برنامجا الاستعراض Firefox وOpera أكتيف إكس، فيمنعان البرامج التي تستغل أكتيف إكس من التأثير على كمبيوترك. كما أن برامج الاستعراض المذكورة أقل عرضة لعمليات الهجوم (بشكل جزئي لأنها ليست واسعة الانتشار مثل إنترنت إكسبلورر، ومبرمجو المالوير يسعون وراء التطبيقات الأكثر استخداماً فيصيبون أكبر قدر ممكن من المستخدمين). وهذا لا يعني أن برامج الاستعراض البديلة لا تحتوي على نقاط خلل. (على سبيل المثال من تموز إلى كانون الأول 2004، تم

الكشف عن 21 نقطة خلل في برامج الاستعراض Mozilla في مقابل 13 نقطة خلل في مايكروسوفت إنترنت إكسبلورر). لذلك إذا كنت تستخدم برنامج استعراض بديل يجب أن تبحث بشكل دوري عن التحديثات الجديدة. وقد تجد أيضاً أن بعض مواقع الوب لا تعمل بشكل جيد مع برامج الاستعراض البديلة.

لكي تحمّل برنامج الاستعراض Firefox، اذهب إلى www.mozilla.org. ولكي تحمل برنامج الاستعراض Opera، اذهب إلى www.opera.com.

حافظ على البرمجيات محدثة

إن تحديث البرمجيات في الكمبيوتر هو ما يكافئ أكل الخضروات: إنها ضرورية من أجل الصحة الجيدة، ويجب أن تنفذ ذلك بشكل دوري. يتم إنشاء برامج السبايوير والأدوير الجديدة بشكل دائم، والأمر كذلك بالنسبة إلى التواقيع التي تكشفها. وهكذا، من المهم أن تحدّث البرمجيات الأمنية. تسمح معظم البرامج بتسليم التحديثات بشكل تلقائي عبر الإنترنت.

ينطبق الأمر نفسه على نظام التشغيل والتطبيقات. كما ذكرنا سابقاً، تصدر مايكروسوفت تحديثات جديدة، تدعى أيضاً الرقع، في ثاني ثلاثاء من كل شهر. يخبرك الفصل السابع كيف تعد الكمبيوتر لكي تحصل على تحديثات مايكروسوفت بشكل تلقائي. ويصدر بائعو المنتجات الأخرى تحديثات برمجية لتغطية نقاط الخلل التي قد تسمح للمهاجم بإيذاء أو السيطرة على كمبيوترك.

5-5 إزالة السبايوير، الأدوير وأحصنة طروادة

إذا اتبعت جميع الخطوات الوقائية المذكورة هنا، يمكنك أن تبقي معظم السبايوير وأحصنة طروادة بعيداً عن كمبيوترك. لكن يظل الاحتمال قائماً بأن تخترق بعض البرامج دفاعاتك، لذلك من المهم أن تعرف علامات الإصابة وطريقة إزالة البرمجيات غير المرغوبة.

إن رهانك الأفضل للتخلص من البرمجيات غير المرغوبة هو باستخدام البرمجيات المضادة للسبايوير والأدوات المضادة للفيروسات. تبحث هذه الأدوات في كمبيوترك عن أي أثر لبرنامج سبايوير، أدوير وحصان طروادة معروف. وبمجرد العثور على أي منها، يمكنك أن تختار حذف، إلغاء تأهيل أو أن تترك البرنامج على حاله. ويمكنك أن تزيل السبايوير وأحصنة طروادة يدوياً، باستخدام الأدوات المتوفرة على الإنترنت.

كيف تعرف أن كمبيوترك مصاب

كما مع الفيروسات والديدان، فإن الطريقة الأفضل لمعرفة أن كمبيوترك قد أصيب بسبايوير، أدوير أو حصان طروادة هو أن تستخدم برمجيات مضادة للسبايوير ومضادة

للفيروسات. تكشف هذه البرامج عن وجود البرمجيات غير المرغوبة على كمبيوترك وتقدم خيارات للتعامل معها. يجب أن تمسح كمبيوترك بشكل دوري بكلا النوعين من البرمجيات وتتأكد من أن برمجياتك الأمنية مؤهلة عندما تتجول على الإنترنت.

إذا لم تكن تملك برمجيات مضادة للسبايوير، فيمكنك الحصول على مسح مجاني من مختلف باعة البرمجيات المضادة للسبايوير. تقدم Webroot Software مسح مجاني يدعى Spy Audit، يمكن العثور عليه في صفحة البدء في موقع الشركة www.webroot.com. وتقدم Zone Labs في الموقع www.zonelabs.com، وSymantec في الموقع www.symantec، أيضاً عمليات مسح لبرامج السبايوير. وتقدم Computer Associates مسح مجاني في الموقع www.ca.com. انقر الارتباط Products تحت اللائحة Home and Home Office، ثم انقر eTrust PestPatrol. فتذهب إلى صفحة تشغيل عملية المسح. يمكنك أن تحصل أيضاً على مسح مجاني من Aluria Software بالتحول إلى www.aluriasoftware.com. تستخدم العديد من عمليات المسح تحكم أكتيف إكس، لذلك يجب أن تنقر في الشاشة التنبيهية في برنامج الاستعراض إنرتنت إكسبلورر.

يمكنك أن تبحث أيضاً عن العلامات التالية:

- هل يفيض كمبيوترك بالإعلانات؟
- هل تتغير صفحة البدء باستمرار مع أنك تعيدها إلى صفحتك المفضلة؟
- هل يتم توجيهك إلى مواقع بحث غير مألوفة و لم تطلبها؟
- هل يعمل كمبيوترك ببطء، خصوصاً عند التجول في الوب؟ تستخدم برامج السبايوير والأدوير التي تتعقب نشاطاتك وصلة الإنترنت لإرسال تقارير وتوجيه الإعلانات إلى كمبيوترك. فتستغل بذلك عرض المجال وتؤثر على سرعة تسليم مواد الوب. كما تستخدم برامج السبايوير والأدوير أيضاً وحدة المعالجة المركزية في الكمبيوتر (CPU). إذا وصل عدد كاف من برامج الأدوير والسبايوير إلى كمبيوترك، فإن هذه البرمجيات تتنافس على طاقة المعالجة مع التطبيقات الأخرى وتؤثر على السرعة الإجمالية التي ينجز بها الكمبيوتر الوظائف المعتادة. وفي العديد من الحالات، تصبح الكمبيوترات المصابة غير قابلة للعمل.
- هل يتوقف كمبيوترك عن العمل مراراً؟
- هل تنبثق الإعلانات على كمبيوترك حتى لو لم تكن موصولاً بالإنترنت؟
- هل تشاهد شريط أدوات جديد في برنامج استعراض الوب؟
- هل حمّلت أنت أو أي شخص يستخدم الكمبيوتر برامج مجانية مثل برمجيات مشاركة الملفات، برامج الطقس، شاشات التوقف أو أدوات تدّعي بأنها تحسن استعراض للوب؟
- هل يكشف جدار النار برامج على كمبيوترك تحاول الوصول إلى الإنترنت؟

استخدام HijackThis

لكي تزيل يدوياً البرامج غير المرغوبة من كمبيوترك، يجب أن تحذف الملفات وإدخالات المسجل التي تنشئها هذه البرامج. يتطلب ذلك أن تعرف التغييرات التي أجرتها برامج السبايوير على مفاتيح المسجل الموجودة ومفاتيح المسجل الجديد التي تم تثبيتها.

توجد أداة شائعة لإزالة قرصنة برنامج الاستعراض من المسجل وهي HijackThis. تمسح هذه الأداة المسجل وتعطيك لائحة (تدعى سجل) بالمحتويات. فيمكنك أن تقرر عندئذ أي المحتويات ستزيلها. تجد نسخة من HijackThis في موقع مبرمجها: www.merijn.org/downloads.html. (وهو مبرمج CWShredder، أداة شائعة لإزالة CoolWebSearch أحد أكثر برامج السبايوير عناداً وسرعة في التطور على الإنترنت. تتوفر الأداة CWShredder مجاناً في الموقع www.merijn.org/downloads.html).

> HijackThis أداة يدوية، أي يجب أن تزيل البرامج غير المرغوبة بنفسك. وعلى العكس من معظم البرمجيات التجارية المضادة للسبايوير، فإن HijackThis لا تقدم نصيحة حول البرامج التي يجب أن تزيلها. وينصح بشدة أن تحصل على المساعدة في اتخاذ القرار بشأن أجزاء المسجل التي ستزيلها. فإذا ارتكبت خطأً عند تغيير المسجل، لن يعمل كمبيوترك بشكل سليم. إذا كان لديك عقد دعم تقني مع شركة AV أو مضادة للسبايوير أو مع مصنّع كمبيوترك، فقد يساعدوك على العمل مع سجل HijackThis.

كحل بديل، يمكنك أن تحصل على المساعدة المجانية للعمل مع السجل HijackThis في عدد من المنتديات على الوب. يدير هذه المنتديات على الوب عدد من المستخدمين الخبراء الذين بإمكانهم مساعدتك في قراءة السجل وإجراء التغييرات. وأحد المنتديات الشهيرة هو CastleCops. اذهب إلى www.castlecops.com وانقر الزر Forums قرب أعلى الصفحة ثم مرر إلى الأسفل إلى القسم Privacy وانقر الإدخال HijackThis - Spyware, Viruses, Worms, Torjans Oh My!، كما هو مبين في الشكل 5-6. تأكد من قراءة توجيهات استخدام المنتدى ووضع السجلات HijackThis. يقدم CastleCops أيضاً دورة تعليمية تقنية عن HijackThis في http://castlecops.com/HijackThis.html.

يوجد خيار آخر هو SpywareInfo، في الموقع www.spywareinfo.com. يمكنك أن تمرر إلى الأسفل في صفحة البدء لكي تبحث عن قسم يدعى The Browser Hijacker Articles. تقدم الارتباطات في هذا القسم معلومات عن طريقة استخدام HijackThis. ويمكنك أن تسجل أيضاً لتضع سجلك أو تطرح سؤالاً في منتدى المستخدمين. وتقدم أيضاً ارتباطات إلى منتديات أخرى على الوب حيث يمكنك مراجعة سجلك HijackThis.

Privacy				
General Privacy Privacy related discussions. Moderators Administrators, Moderators, Forums Admin	ATOM XML	405	[illegible]	[illegible]
Hijackthis - Spyware, Viruses, Worms, Trojans Oh My! Welcome to the HijackThis forum where you can post your HijackThis logs for help from the experts. Moderators Administrators, Moderators, Forums Admin	ATOM XML	[illegible]	262965	Tue May 24, 2005 [illegible]
Phishing, Fraud and Dastardly Deeds Scams involving anything, for example, phishing email scams. Moderators Administrators, Moderators, Forums Admin	ATOM XML	[illegible]	[illegible]	Mon May 23, 2005 [illegible] pm
Spam Topics on Spam: unsolicited commercial email (UCE) and unsolicited bulk email (UBE). Moderators Administrators, Moderators, Forums Admin	ATOM XML	[illegible]	[illegible]	[illegible]

الشكل (6-5): منتدى HijackThis لـ CastleCops.

يمكنك أن تضع السجلات أيضاً في Spyware Warrior (www.spywarewarrior.com). وتحصل على مساعدة إضافية مع السجلات HijackThis في الموقع www.merjin.org.

تنسيق محرك القرص الصلب

في السيناريو الأسوأ، لن تتمكن البرمجيات المضادة للسبايوير من إزالة البرامج غير المرغوبة، وسوف تحتاج إلى طلب المساعدة الخارجية. إذا كنت قد اشتريت برمجيات مضادة للسبايوير، اتصل بقسم دعم الزبائن لتعرف ما يوصون به (لكن استعد لفترة انتظار طويلة). يمكنك أن تتصل أيضاً بمصنّع كمبيوترك، اطلب المساعدة من المخزن الذي اشتريت الكمبيوتر منه (بالطبع لقاء أجرة) أو اتصل بورشة إصلاح كمبيوترات محلية.

وكحل أخير، يمكنك أن تبدأ من البداية وتعيد تثبيت نظام التشغيل والتطبيقات باستخدام أقراص البرمجيات الأصلية. لكي تنفذ ذلك، أدخل نظام التشغيل الأصلي في محرك الأقراص المضغوطة وشغّل الكمبيوتر. يطلب منك الكمبيوتر التأكيد بأنك تريد إعادة تثبيت نظام التشغيل. على كل حال، تمسح عملية إعادة تثبيت نظام التشغيل جميع البيانات التي حفظتها على كمبيوترك (لنفترض أنك تحفظ الملفات احتياطياً بشكل دوري). الحل الأخير: حاول أن تستنفذ الخيارات الأخرى قبل أن تعيد تنسيق محرك القرص الصلب.

6-5 لائحة التدقيق

استخدم هذه اللائحة كدليل مرجعي للمواد المغطاة في هذا الفصل.

ما يجب أن تفعله

- استخدام البرمجيات المضادة للسبايوير، والمحافظة على تحديثها.
- ضبط إعدادات برنامج الاستعراض لكي يتم إعلامك عند تحميل أكتيف إكس.
- قراءة الاتفاقية EULA قبل تحميل أي برمجيات.

- الاشتباه بالبرمجيات المجانية.
- المحافظة على تحديث التطبيقات ونظام التشغيل.
- إنجاز عمليات نسخ احتياطي للملفات الأساسية بشكل دوري.

ما يجب أن لا تفعله

- قبول تحميل البرمجيات غير المطلوبة.
- النقر على الإعلانات المنبثقة أو غير المطلوبة والإعلانات المنبثقة التنبيهية التي تدّعي أنــه يوجد في كمبيوترك برامج سبايوير أو أي مشاكل أخرى.
- قبول ملحقات البريد الإلكتروني من الغرباء.
- فتح رسالة البريد الإلكتروني التي تدّعي أنها صادرة عن معهد مالي أو موقع تجارة إلكترونية ليس لديك عمل معه.
- قبول البرمجيات بدون قراءة الاتفاقية EULA.
- الخشية من تجريب برنامج استعراض جديد.

7-5 موارد مساعدة

يقدم هذا القسم موارد إضافية لمساعدتك على تعلم المزيد.

إن Ben Edelman هو طالب حقوق في جامعة هارفارد وباحث في الرسائل المضــادة للسبايوير. يوجد في موقع الوب الخاص به كثير من المعلومات الجيدة عن الممارسات المخادعة لبائعي الأدوير، طريقة استغلال البرامج للثغرات الأمنية، وانتقادات تشريعات الأعمال المضادة للسبايوير. يمكنك أن تقرأ هذه المواضيع في الموقع www.benedelman.org.

ويقدم الموقع Spyware Warrior معلومات عن كل ما يتعلق بالســبايوير، ويشــغله Eric Howes. إذا كنت تبحث عن منتج سبايوير، دقق الارتباط الذي يقارن بــين مختلــف البرمجيات المضادة للسبايوير، بما في ذلك المنتجات المجانية. يأخذك الارتباط إلى Spyware إلى سجل وب مع العديد من المعلومات حول برامج السبايوير والتطورات الجديــدة في مجتمــع البرمجيات المضادة للسبايوير. ويمكنك أن تنضم إلى العديد من المنتديات وتضــع الســجلات HijackThis. اذهب إلى www.spyware.com.

تقدم PC Pitstop أدوات تشخيصية للكمبيوترات وتقدم معلومــات مفيــدة حــول السبايوير. على سبيل المثال، انظر إلى ترتيبها في أول 25 موقع لبرامج السبايوير والأدويــر في http://www.pcpitstop.com/spycheck/top25.asp.

Merijn Bellekom مبرمج HijackThis، CWShredder وأدوات أخرى مضــادة

للسبايوير، يمكن تحميلها من الموقع www.merijn.org.

الموقع Spywareinfo.com مليء بالمعلومات الجيدة. إذا رغبت بتعلم المزيد عن السبايوير، الكعكات، قرصنة برامج الاستعراض والمزيد، انقر على الزر More Links في صفحة البدء. ويوصي أيضاً بمنتجات لمساعدتك بالتعامل مع البرمجيات غير المرغوبة. إذا سجلت في هذا الموقع، يمكنك أن تضع أسئلة على لوح الرسائل وتحصل على المساعدة مع مشاكل السبايوير (لكن يجب أن تقرأ الأسئلة المتكررة FAQ أولاً). ويمكن أن تشترك بالرسالة الإخبارية التي يكتبها Mike Healan، صاحب الموقع.

لكي تقرأ نسخة من تقرير FTC آذار 2005 عن السبايوير اذهب إلى www.ftc.gov/os/2005/03/050307spywarerpt.pdf. ولكي تسجل شكوى عن سبايوير أو أدوير إلى اللجنة FTC، اذهب إلى www.ftc.gov وانقر الارتباط File a Complaint في صفحة البدء. يمكن أن تتصل أيضاً بالرقم 877-FTC-HELP (877-382-4357).

يوجد في Spywareguide.com قاعدة بيانات ببرامج السبايوير والأدوير المعروفة. يمكنك إدخال اسم برنامج في شريط البحث في صفحة البدء فترى البرنامج مذكوراً. ويرتب الموقع أيضاً برامج السبايوير حسب مستوى الخطر من 1 إلى 10، مع شرح لكل مستوى.

قراءة المادة الغامضة

تقدم kazaa، التي تصدر البرمجيات ند إلى ند لمشاركة الملفات عبر الإنترنت، برامج الأدوير في النسخة المجانية من منتجها. وبالطبع فإن البرمجيات مجانية لكي توافق على وجود الأدوير التي تولد الإعلانات الموجهة.

تشرح الشركة ذلك في الاتفاقية EULA، التي يمكنك أن تقرأها في www.kazaa.com/us/terms2.htm. توجد الأقسام حول الأدوير في أسفل EULA في القسم 9. في منتصف العام 2005، حزمت Kazaa خمسة برامج أدوير بما في ذلك Cydoor، برنامج تسليم إعلانات "يستخدم، حسب Kazaa EULA، وصلة الإنترنت لدى المستخدم لتحديث اختياره من الإعلانات المتاحة وحفظها على محرك القرص الصلب".

وتضم أيضاً GAIN AdServer، "يحدد، حسب Kazaa EULA، اهتماماتك اعتماداً على استخدامك للكمبيوتر ويستخدم هذه المعلومات لتسليم الرسائل الإعلانية إليك".

وتضم Kazaa EULA، ارتباطات إلى EULA لـــ Cydoor وGAIN AdServer وتقول أنه بتحميل Kazaa فإنك تصرح بقبول EULA لكـــل مـــن هـــذه المكونـــات البرمجية.

بالإضافة إلى ذلك تصرح EULA أنك لن تستخدم أي من البرمجيات الأخرى لكي تلغي تأهيل أو لتحجز أي من الإعلانات التي تدعمها هذه المكونات. وإذا أزلت أي مـــن هذه المكونات، تتوقف Kazaa عن العمل.

فإذاً ما العمل إذا كنت تريد حقاً برمجيات مشاركة الملفات المجانية؟ يجب أن تقرر ما تريده من هذه المقايضة. طالما أنك تتحمل النتائج التي يسببها الأدوير (الإعلانات المزعجة، الأداء الضعيف على كمبيوترك، وأي نقاط خلل تظهر عند وجود الأدوير على كمبيوترك)، يمكنك أن تحمّل البرمجيات وتبدأ بمشاركة الملفات.

الفصل السادس

فقط قل لا للسبام

يوجد للسبام هدف واحد: جلب الأرباح للأشخاص المشكوك بأخلاقهم. وكما مع أدوير وسبايوير عالي الخطورة، فإن محاربة السبام هو أمر صعب لأن معظم مرسلي السبام يملكون دوافع مادية تجعلهم يقاومون ويبدعون. وتكون النتيجة هي لعبة مستمرة بين مؤيدي السبام والذين يحاربون السبام. فعلى الجانب الأول، يحاول مرسلو السبام كل شيء: التعامل مع أنظمة البريد الإلكتروني، محاولات معقدة تقنية لاختراق مرشحات السبام، وفيض هائل من البريد التافه يحاول أن يغمر الدفاعات. وعلى الجانب الآخر، يتم تطوير تقنيات جديدة وتحسينها لصد البريد التافه، ويتم نص القوانين لملاحقة ومحاسبة مرسلي السبام، ويصبح المستخدمون أذكى في التعامل مع السبام.

عندما بدأت الإنترنت بجذب الاهتمام بشكل كبير، أعاق السبام عمليات البريد الإلكتروني وقضى عليها تقريباً. وفي هذه الأيام يشكل السبام مصدر إزعاج كبير. وبفضل جهود مطوري البرمجيات، مزودات الخدمة، والمجتمع المضاد للسبام بشدة، يتم إبقاء معظم رسائل السبام خارج صندوق البريد. وتضمن مزودات خدمة الإنترنت (ISP) مثل AOL وComcast، ومزودات بريد الوب مثل !Yahoo، MSN وGoogle أن يحصل مستخدميها على بريد نظيف. ويتم إرسال الرسائل المشبوهة إلى مجلدات بريد خاصة لكي تراجعها، ومن الواضح أنه يتم القضاء على السبام عند عدم تسليمه.

ولكن السبام لا يبدي أي تراجع. فمن أجل كل تقدم محقق في التقنية المضادة للسبام يتم تحقيق تقدم في تقنيات إرسال السبام. يتم إرسال 30 بليون رسالة إلكترونية في اليوم تقريباً عبر الإنترنت، وتنص التقديرات المحافظة على أن 50 بالمائة من هذه الرسائل هي سبام. (ترفع بعض التقديرات نسبة السبام إلى 90 بالمائة من مجموع رسائل البريد الإلكتروني). قد تظن أنك غير معني بالأمر طالما أن البريد التافه لا يجد طريقه إلى صندوقك البريدي. ولكن بالفعل تسبب 15 بليون (أو أكثر) من الرسائل التافهة كلفة كبيرة على مؤسسات الاتصالات ومزودات

الخدمة. فكل رسالة تافهة تعبر الإنترنت تستهلك موارد الإنترنت، مثل عرض المجال على خطوط النقل البحرية وإمكانيات المعالجة للموجهات وملقمات البريد التي تمرر الرسائل من قفزة إلى تالية. كما أن مؤسسات الاتصالات ومزودات الخدمة تستثمر في البرمجيات لكي تعالج وتحلل الرسائل الواردة، ويتوجب عليها شراء كميات كبيرة من العتاد لاستيعاب هذا الحجم الهائل من البريد. وفي النهاية يتحمل المستخدم الكلفة الزائدة على شكل أجرة شهرية أعلى.

يمكن أن يستخدم مبرمجو السبام بأعداد كبيرة تقنيات إرسال السبام بأعداد كبيرة، فهم يبحثون دوماً عن طرق جديدة لزيادة انتشار رسائلهم. هناك إصدار جديد من السبام يدعى التصيد ويرسل رسائل إلكترونية بأعداد كبيرة لخداع المستخدمين وكشف معلومات الحسابات المصرفية. وهكذا، السبام لم يعد مزعجاً فقط: بل يمكن أن يشكل خطراً أيضاً.

ولن تنتهي المشكلة طالما هناك بقي شرطان محققان. الأول، قدرة مرسلو السبام على الاختفاء بسهولة. وبفضل تقنيات إخفاء مصدر البريد الإلكتروني يمكن لمرسلي السبام تمويه مصدر البريد التافه. والإنترنت مليئة بالكمبيوترات غير المحمية، سواء ملقمات بريد أم كمبيوترات منـزلية، والتي يستطيع مرسلو السبام قرصنتها واستخدامها كمولدات سبام بدون علمها. والعالم مليء بمزودات الخدمة التي ترغب بالنظر إلى الزبائن الذين يرسلون آلاف أو مئات الآلاف من الرسائل في اليوم بطريقة أخرى طالما أن فواتيرهم مدفوعة.

والشرط الثاني، هو أن السبام سوف يقاوم طالما الأشخاص الساذجون يستجيبون ويشترون المنتجات والخدمات المعلنة أو يقعون ضحايا للخداع. يذكر هذا الفصل ملخصاً عن اقتصاديات السبام، معلومات عن عمل مرسلو السبام، الأدوات المستخدمة لمحاربة السبام، قسم عن الأعمال الداخلية في البنية التحتية للبريد الإلكتروني، ونصائح مفيدة تقيك من الوقوع ضحية للبريد التافه. سوف ننظر أيضاً إلى عدة منتجات تساعد بمنع وصول السبام إلى كمبيوترك.

1-6 تحقيق الأرباح من السبام

إن السبام هو لعبة نقود ولذلك فهو يخضع للمبادئ الاقتصادية البسيطة: طالما أن السبام يحقق نقوداً أكثر من كلفة إرساله، فسوف يظل موجوداً. فالسبام هو أرخص أشكال الإعلان. إذا أردت أن تبيع حبوب تخفيف الوزن السحرية بأية طريقة أخرى، فسوف تتحمل نفقات إضافية للإعلان. أما عند إرسال 100000 رسالة بريد إلكتروني في اليوم فإنها تكلف أكثر بقليل من كلفة وصلة الإنترنت، بضعة كمبيوترات، وبعض برمجيات السبام الجاهزة (نعم، يمكنك أن تشتري برمجيات السبام – على الإنترنت بالطبع).

يحقق مرسلو السبام أرباحاً كبيرة. لنأخذ كمثال مرسل السبام جيرمي جينـز. لقد تم الحكم عليه بتسع سنين في السجن في تشرين الثاني 2004 لإرساله كميات كبيرة من البريد

الإلكتروني غير المرغوب وتضليل معلومات التوجيه على رسائل البريد الإلكتروني لمنع مستلمي الرسائل من تحديد المرسل. لقد ارتكب جينز عدة أنواع من جرائم السبام بما في ذلك استخدام الصور الفاضحة، برمجيات الخصوصية، ومخطط العمل من المنزل. ووفقاً لمستندات المحكمة، فإن عمليات إرسال البريد الإلكتروني بأعداد كبيرة التي نفذها جينز قد حققت عمليات بيع باستخدام 10000 بطاقة تقريباً في الشهر. وقد طلب حوالي ثلثي الأشخاص الذين اشتروا المنتجات إعادة نقودهم، واستمر جينز بتحقيق ربحاً صافياً أكثر من 100000$ في الشهر. وقد ذكر القضاة بأن الربح الصافي الإجمالي لجينز يقدر بحوالي 24 مليون دولار.

بالطبع لكي يتم تحقيق الأرباح من السبام، يجب أن يوجد باعة ومشترون. والسبب الوحيد لاستمرار وجود السبام هو وجود شخص ما في مكان ما يشتري شيء ما تم الإعلان عنه باستخدام البريد التافه. يمكن أن يكون هذا هو الجانب غير القابل للحل من مشكلة السبام. يمكن تعديل برمجيات ترشيح السبام باستمرار، لكنه يبدو أن السذاجة (أو الغباء ببساطة) هي مشكلة دائمة. وبالفعل فإن عدد الأشخاص الذين يستجيبون للسبام يفوق ما تتخيله. في عام 2004، وجدت دراسة من Pew Internet & American Life Project أن 5 بالمائة من مستخدمي الإنترنت قد اشتروا منتجات تم الإعلان عنها في البريد الإلكتروني غير المرغوب. وفي العام نفسه أصدرت Business Software Alliance نتائج استطلاع تفيد بأنه 21 بالمائة من المشتركين بالاستطلاع قد اشتروا شيئاً ما من إعلانات السبام.

فإذاً ما الذي يجعل الأشخاص يستجيبون إلى عروض السبام؟ أنا لست طبيباً نفسياً، ولكن توجد نظريتان:

- يخاطب السبام رغبات الإنسان الأساسية. فالسبام يتناول عادةً ثلاث رغبات: الجنس (الصور الإباحية، الفياغرا)، المال (المشاريع الهرمية، البرمجيات الرخيصة، خطط أموال النفط النيجرية)، وتحسين الصورة الذاتية (تخفيف الوزن، تضخيم الأعضاء التناسلية، وبضاعة رخيصة من مصمم مشهور). بالفعل، فإن الأزرار التي يحاول مرسلو السبام أن يضغطوها لا تختلف كثيراً عما يستخدمه المعلنون بشكل عام. فمرسلو السبام والتجار يحققون أرباحاً من انشغالنا بتخفيف أعبائنا المادية، تحسين صورتنا الذاتية، وزيادة قدرتنا الجنسية. والأمر الذي يميز مرسلي السبام أنهم يعلنون بشكل رخيص، يصعب تعقبهم، طرقهم غير قانونية على الأغلب وسوف يسرقونك غالباً.
- يوفر السبام المجهولية . فالشخص الذي يرغب بشراء مواد إباحية أو طقم تضخيم الأعضاء التناسلية قد يعجبه المجهولية التي توفرها الإنترنت. فهو غير بحاجة لأن يطلب من طبيبه وصفة للفياغرا بل يحصل عليها بفضل السبام. والشخص الذي يرغب بالحصول على برمجيات مكسورة قد يشعر براحة أكبر بتنفيذ ذلك على الإنترنت. ويمكن لشاشة الكمبيوتر ووسط اتصالات الإنترنت الذي يبدو غير ملموساً أن يقضي على الخجل.

2-6 السبام، الخداع والتصيد

يستمر وجود السبام التقليدي (أعني بتقليدي البريد الإلكتروني غير المطلوب الذي يحاول أن يبيعك شيئاً)، ويعتمد المجرمون أيضاً على إصدارات السبام لخداع المستلمين بـــالوقوع في مختلف عمليات الخداع. الخدعة الأكثر شهرة هي خدعة النفط النيجري، حيث يدعي مرسل السبام بأن لديه ملايين الدولارات يحاول نقلها إلى خارج أفريقيا. (تدعى هذه الفئة أحيانـــاً بالخدعة 419 وهو الرمز الجنائي النيجيري). يعد المرسل بنقل حصة كبيرة مـــن النقـــود إلى حسابك المصرفي، ولكن قبل ذلك يجب أن ترسل بعض النقود من أجل دفع الأجور والأمور الأخرى. هناك خدعة بريد إلكتروني مشهورة أخرى هي اليانصيب الدولي – يمكنك أن تجمع أرباحك بعد أن تدفع أجرة إدارية صغيرة (لن تحصل على شيء بعد ذلك). إن جوهر هـــذا النوع من الخدع (وهناك العشرات منها) هو أنك تعتقد بأنك ستحصل على شـــيء بـــدون مقابل. والحقيقة هي العكس تماماً.

النوع الثاني من السبام والأخطر بكثير يدعى التصيد. تحدث الفصل الثاني، "منع ســـرقة الهوية" عن التصيد، لكن سوف نراجعه هنا إذا كنت قد تجاوزت ذلك الفصل.

تبدأ عمليات هجوم التصيد برسائل بريد إلكتروني (بأعداد كبيرة)، تدعي أنها نموذج مصرفي، شركة بطاقات اعتماد، مزود ISP أو شركة تجارة إلكترونيـــة (eBay وPayPal همـــا هـــدفان شائعان). بعض رسائل التصيد تكون خدع واضحة، ولكن بعضها الأخر هو عمل فني كامل مـــع شعار الشركة ومكتوب بلغة شركات التسويق. يبين الشكل 6-1 مثالاً جيداً عن النوع الثاني.

From: "PayPal" <service@paypal.com> Add to Address Book
To: aconrymurray@yahoo.com
Subject: PayPal Account Security Measures
Date: Tue, 15 Feb 05 22:25:34 GMT

Dear PayPal Member,

Your account has been randomly flagged in our system as a part of our routine security measures. This is a must to ensure that only you have access and use of your PayPal account and to ensure a safe PayPal experience. We require all flagged accounts to verify their information on file with us. To verify your information at this time, please visit our secure server webform by clicking the hyperlink below

Click here to verify your information

Thank you for using PayPal!
The PayPal Team

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

Protect Your Account Info

Make sure you never provide your password to fraudulent websites.

To safely and securely access the PayPal website or your account, open up a new web browser (e.g. Internet Explorer or Netscape) and type in the PayPal URL (http://www.paypal.com/).

PayPal will never ask you to enter your password in an email.

For more information on protecting yourself from fraud, please review our Security Tips at http://www.paypal.com/securitytips

الشكل (6-1): رسالة بريد إلكتروني مزورة.

بشكل عام، تنقل رسالة التصيد تنبيهاً بحدوث خطأ في حسابك ويجب تصحيحه فوراً. وتضم رسالة البريد الإلكتروني ارتباطاً إلى صفحة التوقيع في موقع الوب. إذا نقرت الارتباط، سوف تجد صفحة تسجيل دخول تبدو بشكل مطابق لما هو موجود في الموقع النظامي، مع الحقول كاملة لإدخال اسم المستخدم، رقم الحساب وكلمة المرور. كما تطمع الكثير من المواقع الخادعة وتسأل عن معلومات أخرى، مثل رقم الضمان الاجتماعي. وتقوم الضحية بكتابة المعلومات والضغط على الزر Send بمنتهى الحس بأداء الواجب وتصحيح أي مشاكل في الحساب. فيتم سرقة معلومات الحساب.

لا يكتفي مستخدمو خدعة التصيد بذلك، بل يضم العديد منهم برامج خبيثة في رسالة البريد الإلكتروني التي أرسلوها أو على موقع الوب الذي أرسلوه، مثل الفيروسات، مسجلات ضربات المفاتيح أو أحصنة طروادة. (انظر إلى الفصل الرابع، "التخلص من الضيوف غير المرغوبين، الجزء 1" والفصل الخامس، "التخلص من الضيوف غير المرغوبين، الجزء 2"). في بعض الحالات، يكون مجرد فتح رسالة البريد الإلكتروني كافياً لكي يحمل برنامج المالوير نفسه على كمبيوترك. وهكذا وحتى لو لم تقع ضحية خدعة التصيد بنفسك، فإن احتمال إصابة كمبيوترك قائمة.

3-6 كيف يعمل مبرمجو السبام

يستخدم مرسلو السبام مختلف الطرق في سبيل نجاح تجارتهم. بعض هذه الطرق معقدة تقنياً وتتضمن التعامل مع بروتوكولات الإنترنت المستخدمة لتسليم وتعقب البريد الإلكتروني. وبعضها الآخر بسيط كشراء قرص مضغوط يحتوي على عناوين البريد الإلكتروني. يعمل مرسلو السبام بشكل دائم على إرسال أعداد كبيرة من الرسائل بسبب صعوبة وصول الرسائل عبر المرشحات المختلفة المستخدمة في مزودات الخدمة ولدى المستخدمين. وهكذا يرسل مرسلو السبام ملايين الرسائل على أمل أن يجد 1 أو 2 بالمائة منها طريقه إلى صناديق البريد وأن 1 أو 2 بالمائة من الرسائل الواصلة سوف تحقق مبيعات. يتحدث هذا القسم عن بعض الخدع الشائعة المستخدمة.

شراء اللوائح

الطريقة الأبسط لبدء العملية هي بشراء لوائح عناوين البريد الإلكتروني. على سبيل المثال، تبيعك شركة تدعى Bulk Email Software Superstore أكثر من مليون عنوان بريد إلكتروني لقاء 40$. كما أن عملية بحث بسيطة على الإنترنت سوف تكشف عن عشرات المواقع التي تقدم عروض مماثلة. يمكن أن يشتري مرسلو السبام لوائح بعناوين البريد الإلكتروني المسروقة. وفي حزيران 2004، تم تجريم مهندس برمجيات في AOL بسرقة 92 مليون عنوان بريد إلكتروني لمستخدمي AOL، ثم باعها إلى مرسلي السبام.

زواحف البريد الإلكتروني

توجد برامج على الإنترنت تزحف على صفحات الوب بحثاً عن عناوين البريد الإلكتروني. تمسح هذه الزواحف ملايين الصفحات، وتبحث عن الإشارة @ وتبني قواعد بيانات بعناوين البريد الإلكتروني. تستخدم الشركات ومرسلو السبام هذه الزواحف من أجل تجميع العناوين.

هجوم القاموس/حصاد الدلائل

هجوم القاموس (أو حصاد الدلائل) هو طريقة قسرية لإرسال السبام. ينشئ مرسل السبام برنامجاً يكرر عمله عبر مختلف أشكال الأسماء المعروفة (Jone-Smith@isp.com، J-Smith@isp.com، jsmith@isp.com، Ted-Smith@isp.com) ويختار ميدان معين كهدف، ثم يشغل البرنامج. يرسل البرنامج عندئذ مئات الآلاف أو ملايين من الرسائل الإلكترونية على أمل أنه تكون بعض الأسماء مقبولة ويتم تسليم الرسائل إلى أصحابها. إن هجوم القاموس هو مشكلة جدية لأنه بإمكانه أن يغمر ملقم بريد مستهدف ويستخدم موارده فيصبح دخول البريد النظامي غير ممكناً.

الخداع

يحاول مرسلو السبام كل ما بوسعهم لإخفاء مصدر الرسالة لأن مزودات الخدمة تتحرك بسرعة لحجز مصادر السبام ولأن المرسوم الفيدرالي CAN-SPAM يقضي بحجز مرسلي السبام في السجن إذا تم التقاطهم وتجريمهم.

كما ذكرنا سابقاً، فإن SMTP هو بروتوكول إرسال البريد الإلكتروني. يعتمد SMTP على نوعين من الترويسات لتسليم البريد: ترويسات الغلاف وترويسات الرسالة. يستخدم SMTP ترويسات الغلاف لكي يخبر ملقمات البريد عن وجهة الرسالة. ويضيف كل ملقم بريد تمر الرسالة عبره ترويسة الرسالة الخاصة به. يمكنك أن تعرف التقدم الذي حققته الرسالة في مسارها على الإنترنت بقراءة ترويسات الغلاف. ولكن مرسلو السبام ينشئون أيضاً ترويسات زائفة ويحقنون رسائلهم الإلكترونية في ملقمات البريد لإخفاء مسارها.

تضم ترويسات الرسائل السطرين: To وFrom اللذين تراهما في رسالة البريد الإلكتروني. ويسهل كثيراً تزوير هذه الترويسات. يمكنك أن تنفذ ذلك بنفسك بوضع عنوان بريد إلكتروني زائف في السطر :From.

الملقمات الوكيلة للسبام

الملقمات الوكيلة للسبام هي ملقمات بريد أو كمبيوترات تم قرصنتها لإرسال السبام.

يمكن للملقم الوكيل للسبام أن يكون ملقم بريد تم إعداده بشكل خاطئ كمرسل مفتوح. وفي حالات أخرى، يحاول مرسلو السبام أن يزرعوا برامج أحصنة طروادة على الكمبيوترات. كما تم شرحه في الفصل الخامس، تطرح برامج أحصنة طروادة نفسها كبرمجيات بريئة أو مفيدة، ولكن عند تثبيتها تمنح المهاجم تحكم كامل بالكمبيوتر. على سبيل المثال، في عام 2003 تضمن الإصدار "F" من الفيروس SoBig حصان طروادة يسمح لمرسلي السبام بتحويل الكمبيوتر الذي تم الوصول إليه، إلى مرسل سبام. والكمبيوترات مع الوصلات عريضة المجال هي أهداف شائعة لهجوم الملقم الوكيل للسبام بسبب عرض مجالها الكبير ووصلاتها الدائمة مع الإنترنت.

إن الملقمات الوكيلة للسبام عالية القيمة لدى مرسلي السبام. فهي تبدو أنها مصدر السبام. وعندما يتم وضع الملقم الوكيل للسبام على اللائحة السوداء (أي تمتنع المزودات ISP عن قبول البريد من هذا الجهاز)، يتخلى مرسلو السبام عن الملقمات الموضوعة على اللائحة السوداء بسهولة ويستخدمون ملقمات جديدة.

الهندسة الاجتماعية

بعد أن يحصل مرسل السبام على عنوان بريد إلكتروني، يكتب رسالة جذابة لكي تفتحها. وهنا تدخل الهندسة الاجتماعية في اللعبة. إن الهندسة الاجتماعية هي طريقة لوصف عملية خداع الناس. لا تتعلق بعض رسائل السبام بالهندسة الاجتماعية – فهي تريد أن تعرف أنها تقدم عرضاً لبيع الفياغرا. وبعض مرسلي السبام الآخرين يريدون أن تفتح وتقرأ رسالة البريد الإلكتروني، لذلك يستخدمون ترويسات مواضيع غامضة أو جذابة (مثل Hello!). تعتمد رسائل التصيد بكثرة على الهندسة الاجتماعية وذلك لأن الخدعة تنتهي إذا لم تصدق أنها تصدر عن المؤسسة التي تدعي أنها صادرة عنها.

مرشدات الوب/علل الوب

مرشدات الوب، وتدعى أيضاً علل الوب، هي برامج صغيرة HTML أو GIF (ملف صورة). وعند تأهيلها، تفتح وصلة إلى الملقم لكي تحمّل ملف الصورة. وفي الوقت نفسه، يرسل مرشد الوب معلومات إلى ملقم الوب. يمكن وضع مرشد الوب على صفحة الوب أو في رسالة إلكترونية لتعقب سلوك المستخدم. وتستخدم العديد من مواقع الوب النظامية مرشدات الوب من أجل تحليل سلوك المستخدم والمساعدة بتخصيص جلسة الاستعراض. يضع مرسلو السبام مرشد الوب ضمن رسالة السبام لكي يعرفوا فيما إذا تم فتح الرسالة. ويساعد ذلك مرسلي السبام على فصل العناوين "الحية" عن العناوين التي لا تستجيب. يمكن أن تكون مرشدات الوب صغيرة كبكسل واحد بحيث يستحيل على عين الإنسان أن تلاحظها.

4-6 طرق ترشيح السبام

إن الحاجة هي أم الاختراع، وهذه هي الحال تماماً مع المرشحات المضادة للسبام. وخلال السنوات التي كان يعمل فيها باحثو البرمجيات المضادة للسبام، تطورت طرق الترشيح من عمليات بسيطة للبحث عن الكلمات الأساسية إلى أدوات تحليل إحصائية معقدة تعتمد على أبحاث في الذكاء الصنعي. وكانت النتيجة هي مجموعة أدوات متكاملة تقدمها المنتجات المضادة للسبام للمساعدة بكشف وإزالة السبام.

جميع هذه الأدوات مؤتمتة؛ أي أن برنامج الكمبيوتر يتحرى الرسائل الواردة ويقرر فيما إذا كانت سبام أو هام (تعني "هام" رسائل مطلوبة). على كل حال، تخاطر أدوات الترشيح المضادة للسبام باحتمال تحديد الرسالة بشكل خاطئ. إن تسمية رسالة مطلوبة بسبام يدعى كشف خاطئ. وتسمية رسالة سبام كهام يدعى عدم الكشف. ويوجد للتسمية الخاطئة نتائج على المستخدم يجب أن يطلع عليها. فالكشف الخاطئ يسبب دخول رسالة سبام إلى صندوق بريدك. أما عدم الكشف فيؤدي إلى عدم استلام رسالة مطلوبة نهائياً.

يمكن ضبط طرق الترشيح المذكورة هنا للوصول إلى توازن بين زيادة كشف السبام وتقليل الكشف الخاطئ. تميل مزودات البريد الإلكتروني الرئيسية مثل Yahoo! وAOL إلى أنه تكون محافظة بدرجة أكبر قليلاً؛ أي أنها تتحمل خطر تسليم نسبة مئوية من السبام أعلى بقليل لكي تضمن تسليم جميع رسائل البريد النظامي. لذلك فإن معظم مزودات البريد الإلكتروني تستخدم مجلد بريد كبير لكي تتجنب الوقوع في هذه المشكلة. يضع الكمبيوتر الرسائل التي لا يمكن تصنيفها في هذا المجلد من أجل اتخاذ قرار نهائي بشأنها.

تستخدم التقنيات الواردة في بقية هذا القسم بشكل عام من قبل مزودات الخدمة، الأعمال ومديري ملقمات البريد الصغيرة. كما يستخدم بعضها في المنتجات المضادة للسبام لدى المستخدم. وإذا كنت تنفذ مرشح بريد شخصي لمستضاف البريد الإلكتروني لدى المستخدم، فإن هذه اللائحة تساعدك على فهم الأدوات المستخدمة لإبعاد السبام.

مرشحات المحتوى/البحث عن الكلمة الأساسية

تمسح مرشحات الكلمة الأساسية أسطر الموضوع وجسم الرسالة بحثاً عن الكلمات والجمل التي تشير إلى أن الرسالة سبام. البحث عن الكلمة الأساسية هو أحد أقدم وأبسط الطرق المعروفة لمحاربة السبام. كما أنها الأقل فعالية. يؤمن البحث عن الكلمة تحكماً دقيقاً بلوائح الكلمات، ولكن احتمال الكشف الخاطئ يصبح كبيراً. على سبيل المثال، إذا كانت الكلمة "breast" ممنوعة، فقد يحجز البحث عن الكلمة الأساسية رسالة إلكترونية حول سرطان الثدي breast cancer أو حول مواضيع أخرى غير مؤذية. وبالإضافة إلى ذلك، يسهل على مرسلي السبام الالتفاف حول مرشحات البحث عن الكلمة. فالعديد من أدوات

السبام تخطئ عمداً في كتابة الكلمات فتمر عبر المرشح لكن الدماغ البشري يظل قادراً على فهمها، ككتابة الكلمات "porn" باستخدام الصفر بدلاً من الحرف "O" (p0rn). وينطبق الأمر نفسه مع الكلمة Viagra والعدد الكبير من الأشكال المختلفة لكتابة هذه الكلمة، بحيث يمكن وضعها في قاعدة بيانات وتحميلها في ملقم البريد. وتنجز أدوات السبام خدعاً أخرى، كإدراج تعليقات HTML بين حروف الكلمة. فشيفرة HTML غير مرئية للشخص الذي يقرأ الكلمة، وبذلك يتم الالتفاف على المرشح.

اللوائح السوداء

تحجز اللوائح السوداء البريد الإلكتروني الذي يأتي من عناوين IP أو ميادين محددة. يمكن أن تكون اللائحة السوداء التي يتم صيانتها بعناية فعالة جداً في حجز مصادر السبام المعروفة. اللائحة السوداء الأكثر شهرة هي نظام منع إساءة البريد (MAPS، www.mail-abuse.com). لديها قاعدة بيانات بالعناوين IP للقمات البريد المعروفة بأنها جيدة أو على الأقل حيادية بالنسبة لمرسلي السبام، تدعى Realtime Blackhole List (RBL). كما يتم تخديم لوائح سوداء معروفة جيداً في SpamCop (www.spamcop.net) وSpamHavse (www.spamhavse.org). تستخدم هذه اللوائح السوداء مزودات الخدمة، الأعمال، وأي ملقم بريد. يمكن أن يستخدم مزود الخدمة ISP هذه اللائحة السوداء أو غيرها كجزء من خدمة ترشيح السبام.

على كل حال، يمكن أن تكون اللوائح السوداء أداة غير دقيقة. فمرسلو السبام يغيرون بشكل دائم الميادين والعناوين IP، لذلك فإن اللائحة السوداء تتقادم بسرعة. بالإضافة إلى ذلك، قد يعاني الكمبيوتر المصاب أو ملقم البريد الذي تم وضعه على اللائحة السوداء قبل أن يزال اسمه من اللائحة بعد حل المشكلة. وأثناء ذلك، تستمر أي مؤسسة تستخدم قاعدة البيانات بحجز البريد الإلكتروني الصادر عنه ولو لم يكن سبام. إذا صادفت قاعدة بيانات موجهة للمستخدمين، تأكد من تدقيق المعايير المستخدم لإضافة الميادين والعناوين IP إلى اللائحة، سرعة إزالة الميادين، تكرار تحديث اللائحة.

اللوائح البيضاء

إنها مجموعات من الميادين أو عناوين البريد الإلكتروني الموثوقة. فاللوائح البيضاء دقيقة جداً وتكمّل اللوائح السوداء بتقديم تحكم أكثر دقة. ومع أنه يمكن أن تحجز اللائحة السوداء ميداناً عاماً، فإن اللائحة البيضاء تفتح الأجزاء المعروفة من هذا الميدان والتي ترسل بريداً مقبولاً. واللوائح البيضاء مفيدة لأنها تضمن تسليم البريد من المصادر الموثوقة وتدع تلك الرسائل تمر عبر طرق كشف السبام الأخرى، وتوفر بذلك زمن وطاقة المعالجة. وفي الجانب الآخر، تحتاج اللوائح البيضاء إلى صيانة دائمة بإضافة أو إزالة العناوين أو الميادين.

التحليل المساعد

يطبق التحليل المساعد عدد من الاختبارات المختلفة على الرسائل الواردة. تبحث هـــذه الاختبارات عن المميزات التي تدل على السبام. ويساهم كل من هذه المميــزات في علامـــة احتمالية السبام، فتعطى الرسالة علامة احتمال كلية بالاعتماد على نتائج الاختبار. على سبيل المثال، لكي يلتف بعض مرسلو السبام حول ترشيح الكلمة الأساســية، يضـــمنون مراجـــع HTML أو صور في جسم الرسالة. وعندما تفتح البريد (يستخدم غالبـــاً ســـطر موضـــوع مضلل)، يعرض مستضاف البريد الإلكتروني الصورة. وكما قد تتخيل (أو قد رأيت)، فـــإن العديد من هذه الصور هي صور جنسية. يمكن أن يستخدم مرشح التحليل المساعد كشـــف الصورة كأحد الاختبارات. وعند اشتراكها مع أنواع اختبار أخرى، مثل الرسائل التي تضـــم خطوط كبيرة أو نص مدرج بشكل عشوائي، وترويسات مزورة، تحصل الرسالة على معدل احتمالية أعلى من الرسالة التي تقول "mortgage rates" ولكن بدون إطلاق أي تنبيه. وبفضل إعطاء وزن لمختلف المميزات، يزيد التحليل المساعد من الثقة بأن رسالة مع علامة سبام عالية هـــي بريد تافه فعلاً (والعكس بالعكس). توجد أداة شائعة للترشيح المساعد من أجل ملقمـــات البريـــد وهي برمجيات المصدر المفتوح Spam Assassin (http://spamassassin.apache.org/).

على كل حال، يمكن أن تستمر المرشحات المساعدة بتوليد الكشف الخاطئ. بالإضافة إلى ذلك، يجب إجراء اختبارات جديدة لمواجهة تقنيات السبام الجديـــدة، والتخلـــي عـــن الاختبارات القديمة. تستخدم مزودات الخدمة على الأغلب التحليل المساعد كجزء من طقـــم أدوات ترشيح السبام. ويمكن أن تستخدم البرمجيات المضادة للسبام لدى المستخدم التحليـــل المساعد أيضاً.

تواقيع السبام

تستفيد هذه الطريقة من تقنية البرمجيات المضادة للسبام. يحسب البرنامج جمع التدقيق أو المزج المشفر لرسالة سبام معروفة، ثم ينشئ توقيعاً أو بصمة لتلك الرسالة. إن جمع التدقيق أو المزج هو عملية رياضية يمكن أن تحوّل رسالة نصية إلى مجموع رقمي. فإذا أخذت جمع التدقيق لنسختين متطابقتين من الرسالة، سوف تحصل على النتيجة نفسها. ويؤدي أي تغيير على نص الرسالة إلى توليد جمع مختلف. إن طريقة جمع التدقيق رائعة لتحديد رسائل السبام لأن مرسلي السبام يبعثون بآلاف أو ملايين النسخ من الرسالة نفسها. يحفظ المرشح المعتمد على التواقيـــع نسخة عن توقيع رسائل السبام الحالية ثم يطبق جمع التدقيق على الرسائل الواردة. وأي رسالة واردة تطابق توقيعاً تعتبر سبام ويتم استبعادها.

على كل حال، اكتشف مرسلو السبام طريقة للالتفاف على هذه التقنية. على ســـبيل المثال، تدرج العديد من أدوات السبام سلاسل وأرقام عشوائية في نهاية ســـطر الموضـــوع أو

ضمن كل رسالة صادرة. ويدرجون أيضاً تعليقات HTML بين الكلمات والحروف. لا يرى مستلم الرسالة هذه الإضافات ولكنها تدخل في حساب أي جمع تدقيق، إن إدخال عناصر عشوائية ضمن رسالة البريد الإلكتروني يضمن أن تكون نتيجة جمع التدقيق مختلفة للرسائل التي تعطي نتائج مشابهة بدون ذلك.

بالطبع فإن البرمجيات المضادة للسبام تتابع المعركة باستخدام المرشحات المسبقة لعزل الإدخالات العشوائية وحساب جمع تدقيق من أجل مميزات الرسالة المهمة فقط. إن الشرط الحرج على تقنية توقيع السبام هو الوقت: فالتوقيع لن يكون مفيداً إذا وصل السبام إلى صندوقك قبل أن يصل التوقيع إلى قاعدة البيانات.

التحدي والاستجابة

يستفيد نظام التحدي/الاستجابة من كون السبام عملية مؤتمتة بحجر البريد من المرسلين الجدد وطلب إكمال التحدي من الشخص المرسل. فإذا استجاب المرسل إلى التحدي يتم السماح بدخول الرسالة إلى صندوق البريد. أما إذا كانت الرسالة صادرة عن مرسل سبام فإن العنوان :From يكون مزوراً بطريقة ما، لذلك لا يتم الاستجابة إلى التحدي. وحتى لو كان العنوان :From من مرسل السبام مقبولاً، فعلى الأغلب تم إرسالها من برنامج على الكمبيوتر ولذلك لن يعرف طريقة الاستجابة إلى التحدي. في كلتا الحالتين يفشل المرسل أمام التحدي، ويتم استبعاد البريد المرسل.

إن التحدي هو نوع من الأحجية أو الاختبار لا يمكن أن يجتازه إلا الإنسان. أحد أنواع التحدي المشهورة هي عرض أحرف أو أرقام ملتفة أو مبهمة قليلاً ولكن يمكن قراءتها، فيعيد عندئذ الشخص الإجابة الصحيحة على التحدي.

إن المشكلة الرئيسية مع آلية التحدي والاستجابة هي توليد حركة مرور إضافية، ويقلل ذلك من مردود مزودات الخدمة والأعمال التي تحاول أن تخفف من حجم البريد الإلكتروني الضروري لأداء عملها. كما يمكن استبعاد البريد الإلكتروني المقبول إذا لم يستجيب المرسل إلى تحدي البريد الإلكتروني في الوقت المحدد.

ترشيح بايسان

إن ترشيح بايسان هو أحد أشكال تصنيف النصوص التي يمكن تطبيقها على كشف السبام. يتعلم مرشح بايسان أن يميز بين السبام وغير السبام باختبار اللغة المستخدمة في مجموعة من رسائل السبام واللغة المستخدمة في مجموعة من الرسائل النظامية. على سبيل المثال، يمكن أن تظهر العبارة انقر هنا "click here" في 90 رسالة من أصل 100 رسالة سبام. لذلك يسند المرشح علامة احتمال كلية إلى العبارة "click here" كمؤشر للسبام. على الجانب الآخر،

يمكن أن تظهر العبارة "Area 51" في معظم رسائل البريد المقبولة حول UFO. في هذه الحالة، يسند المرشح علامة احتمال عالية بأن وجود العبارة "Area 51" يشير إلى رسالة مقبولة.

عندما تصل رسالة جديدة، يبحث المرشح عن الكلمات أو العبارات التي تملك أعلى علامات الاحتمالية بكونها سبام أو غير سبام. ثم يحسب المرشح علامة الاحتمال بكون الرسالة سبام أو غير سبام باستخدام العلامات المنفردة للكلمات المجمعة.

يجذب مرشح بايسان الانتباه إلى معدلات الكشف المدهشة التي يحققها. يدّعي بيل ييرزونيس، مبرمج مرشح يدعى CRM114 (http://crm114.sourceforge.net)، بتأمين دقة أكبر من 99.9 بالمائة على الرسائل الواردة. ويدّعي بول غراهام، مبرمج مرشح بايسان، بمعدل كشف 99.75 في فترة شهر واحد. كما صرّح عن ثمانية حالات كشف خاطئ من 7000 رسالة مقبولة في تلك الفترة. تصف مقالته "خطة من أجل السبام" ترشيح بايسان بمزيد من التفصيل وتوجد في الموقع http://www.pavlgraham.com/spam.html.

تعمل مرشحات بايسان بأفضل شكل عند تدريبها على رسائل السبام وغير السبام. لاحظ أنه يجب إعادة تدريب مرشح بايسان بشكل دوري لكي يتكيف مع التغييرات الطارئة على السبام. لأنه بدون إعادة التدريب، ينخفض أداء المرشح. ويشترك مرسلو السبام بتسميم بايسان، فيضعون كتل كبيرة من النص العشوائي، مثل مقطع من موسوعة، لكي يزيدوا من علامة الرسالة بأنها غير سبام.

ترشيح السمعة

تتعقب شركات متعددة الميادين والعناوين IP وتعطيها علامة سمعة بالاعتماد على حجم الرسائل المقبولة وحجم رسائل السبام الصادرة عنها. فيمكن إعداد ملقمات البريد عندئذ لتحجز البريد الإلكتروني من أي مصدر سمعة سيئة. تشبه هذه الطريقة اللوائح السوداء، ولكنّ مرشحات السمعة مرنة أكثر. على سبيل المثال، يمكن إزالة الميدان أو العنوان IP من مرشح السمعة بسرعة أكبر عندما يبدأ سلوكه بالتحسن.

تعتمد شركة تدعى Cloudmark على آراء المستخدمين لتفصل السبام عن الرسائل المقبولة. عندما يستقبل أحد المشتركين في Cloudmark رسالة يظن أنها سبام، يخبر Cloudmark عن هذه الرسالة، فتنشئ بصمة عنها. ثم تزن الخدمة دقة المستخدم لكي تقرر حجز الرسالة. تصرح Cloudmark أن لديها أكثر من مليون مستخدم. إذا كنت تستخدم مايكروسوفت أوتلوك أو أوتلوك إكسبريس، يمكنك أن تجرب هذه الخدمة مجاناً في الموقع www.cloudmark.com/safetybar البرنامج Bonded Sender يستخدم طريقة ترشيح السمعة. فالمؤسسات التي ترسل عدد كبير من رسائل البريد الإلكتروني التجارية التي طلبها المستخدمون (مثل الرسائل الإخبارية، البيانات المالية وهكذا) تجد غالباً أن مرشحات السبام

تحجز رسائلها. لذلك يمكن أن تضع هذه المؤسسات رهن مالي عبر البرنامج Bonded Sender، لكي تساعد البريد التجاري المقبول على اجتياز مرشحات السبام. إذا اشتكى مستخدم أن البريد الإلكتروني لم يكن مطلوباً، تخسر المؤسسة مبلغاً يتم تحصيله من نقود الرهن. وفي مقابل هذا الضمان، يسمح مالك مرشح السبام بمرور البريد الإلكتروني من المشاركين Bonded Sender عبر مرشحاته. يتم تمويل البرنامج Bonded Sender من IronPort، والتي تصنع ملقمات البريد الإلكتروني. لا يستطيع المستخدمون المستقلون الانضمام إلى هذا البرنامج، ولكن يمكنك معرفة المزيد عنه في الموقع www.bondedsender.com.

5-6 كيف تخفف من السبام

توجد طرق عديدة لضمان عدم إغراق صندوق بريدك بالسبام. يفضل هذا القسم التقنيات البسيطة التي يمكنك استخدامها وبدون أي كلفة. وتتضمن معظم هذه التقنيات على قليل من الحدس العام. بشكل عام، تعامل عنوان بريدك الإلكتروني بالطريقة نفسها التي تعامل فيها المعلومات الحساسة الأخرى، مثل رقمك الهاتفي. لن توقف هذه التوصيات من تدفق السبام، لكنها تبقي حجمه تحت الحدّ الذي يمكن التحكم به.

احذف الرسائل المشبوهة بدون فتحها

يمكن أن تحدد رسائل السبام، التصيد أو الرسائل الخادعة من المعلومات الموجودة في عنوان البريد الإلكتروني أو سطر العنوان. تساعدك اللائحة التالية بتحديد البريد غير المرغوب. إذا اشتبهت برسالة إلكترونية، يفضل أن تحذفها قبل أن تفتحها. فالعديد من رسائل السبام تستخدم مرشدات الوب، كما شرحنا سابقاً، لتكشف البريد الحي. وبفتح الرسالة يتم تفعيل المرشد وتزداد قيمة بريدك الإلكتروني بالنسبة إلى مرسل السبام. كما أن العديد من رسائل التصيد تحمل الفيروسات أو برامج مالوير الأخرى التي يمكنها أن تهاجم كمبيوترك بمجرد فتح الرسالة. لذلك فإن الطريقة الأفضل هي حذف الرسائل المشبوهة بدون قراءتها.

نذكر بعض الملاحظات لتحديد رسائل السبام والتصيد بدون فتح الرسالة:

- لم تشاهد عنوان البريد الإلكتروني الموجود في الرسالة سابقاً.
- ينتمي ميدان البريد الإلكتروني إلى بلد أجنبي لا يوجد لديك عمل معه.
- تم كتابة النص الموجود في سطر الموضوع بأحرف غريبة (مثلاً VIAGR@).
- يستخدم نص سطر الموضوع لغة غامضة ولكنة تنبيهية (على سبيل المثال، "مستعجل!"، "ملاحظة مهمة!" أو "دعوة").
- يشير نص سطر الموضوع إلى نوع من العرض، الاقتراحات، الترويج التجاري أو الصفقات.

- يستخدم نص سطر الموضوع ":Re" ولغة غامضة مثل "مستندك" أو "كما ناقشنا" لكي تبدو الرسالة وكأنها إجابة إلى رسالة أرسلتها سابقاً. إذا لم تتعرف على عنوان البريـد الإلكتروني أو إلى مضمون المحادثة، فقد تكون خدعة غالباً.
- تتظاهر الرسالة بأنها نموذج من موقع مصرفي أو موقع تجارة إلكترونية ليس لديك عمل معه.

لا تجب على رسائل السبام أو التصيد

إذا فتحت رسالة وتبين أنها سبام، لا تجيب عليها. لأن الإجابة على الرسالة يخبر مرسل السبام بأنه توصل إلى عنوان حي. تدّعي بعض رسائل السبام أيضاً باعتماد سياسة الرفض؛ أي يمكنك الإجابة بأنك لا تريد استقبال مزيداً من الرسائل. وغالباً ما يكون ذلك خدعة، فـإذا طلبت عدم استقبال المزيد من الرسائل، يعرف مرسل السبام بأن هذا العنوان حي.

لا تنقر أي ارتباط في البريد غير الموثوق

إذا فتحت رسالة إلكترونية وما تزال غير متأكداً بأنها حقيقية، لا تنقر على أي ارتبـاط موجود ضمن الرسالة. لأنه يمكن أن تنشط هذه الارتباطات برامج المالوير أو تأخذك إلى موقع وب مقلد. إذا أردت بالفعل أن تتحرى العرض، أغلق الرسالة، افتح برنامج استعراض الوب، واكتب بشكل يدوي العنوان في حقل المحدد URL. يمكنك أن تدقق أيضاً موقع وب مجموعة العمل المضادة للتصيد (APWG)، وهي مؤسسة تعمل على تكوين أفضل الخبرات الصـناعية لصد عمليات هجوم التصيد. تنشئ المجموعة قاعدة بيانات برسائل التصيد لمساعدة المستخدمين على تحديد رسائل البريد الإلكتروني الخادعة. يمكنك أن تجد مجموعة مـن رسـائل التصـيد بالتحول إلى الموقع **www.antiphishing.org** والنقر على الارتباط **Phishing Archive** على الجانب الأيسر من الصفحة.

اقرأ سياسات الخصوصية

قبل أن تبدأ بممارسة الأعمال مع موقع تجارة إلكترونية، من الأفضل أن تقـرأ سياسـة الخصوصية لكي تعرف المعلومات التي تجمعها منك (تطلب معظم المواقع عنوان بريد إلكتروني) وما الذي ستفعله بهذه المعلومات. يجب أن تقدم مؤسسات الأعمال النظامية ارتباطاً واضـحاً إلى سياسة الخصوصية على مواقعها على الشبكة. يجب أن تقدم أيضاً إمكانية رفض اسـتقبال المزيد من البريد الإلكتروني غير المطلوب وعدم بيع الشركة لمعلوماتك إلى المؤسسات الأخرى.

لا تصرح عن عنوان بريدك الإلكتروني

إذا كنت تدخل بشكل متكرر إلى غرف المحادثة وتضع رسائل على ألواح النقـاش، لا تضع عنوان بريدك الإلكتروني. وإذا كان لديك موقع وب، لا تضع عنوان بريدك الإلكتروني

عليه. فمرسلو السبام يستخدمون الزواحف المؤتمتة للبحث في الإنترنت وتجميع عناوين البريد الإلكتروني (بالبحث غالباً عن الرمز @).

غيّر عنوان بريدك الإلكتروني أو استخدم عدة عناوين بريد إلكتروني

إذا أردت أن تصرح عن عنوان بريدك الإلكتروني، يمكنك أن تغيره لكي تصد الزواحف المؤتمتة. هناك خدعتان معروفتان وهما أن تكتب الرمز @ والنقطة (johndoe at isp dot com) أو أن تضيف جملة مثل "no spam" في العنوانjanedo@nospam.isp.com). لن يستطيع أي زاحف يلتقط هذا العنوان أن يسلم رسالة إليه، لكن الإنسان يفهم بأنه يجب إزالة هذه العبارة من العنوان. (إذا كنت قلقاً بأن يظن الناس أن "no spam" تشكل جزءاً من العنوان، يمكنك أن تضع تعليمات حول هذا الموضوع على صفحة الوب).

على كل حال، نادراً ما تضبط برامج السبام أدواتها بشكل كاف لتكشف خدعاً كهذه، لذلك فالخيار الآخر هو استخدام عدة عناوين بريد إلكترونية. على سبيل المثال، يمكنك إعداد عنوان تعطيه إلى العائلة والأصدقاء فقط. ثم تنشئ حسابات إضافية ليستخدمها العموم، لوضعها على الوب أو عند التعامل مع المواقع التي تشتبه بأنها بريدك الإلكتروني.

هناك خيار آخر وهو اختيار عنوان بريد إلكتروني غير واضح. على سبيل المثال، بدلاً من استخدام اسمك الأول وكنيتك (johndoe@isp.com)، جرّب مجموعة من الأحرف والأرقام أو جملة (على سبيل المثال، j225doe@isp.com أو dontpanic@isp.com). يساعد ذلك بمنع سبام القاموس (مع أنه يصبح تذكر العنوان صعباً).

بالإضافة إلى ذلك، تسمح بعض خدمات البريد بإنشاء عناوين يمكن رميها. على سبيل المثال، تسمح الخدمة Yahoo!Mail Plus بإنشاء 500 عنوان ضمن حسابك في Yahoo (هذا الخيار غير متاح مع حساب Yahoo! Mail المجاني). يمكنك استخدام العناوين التي يمكن رميها للتعامل مع مواقع التجارة الإلكترونية، والمشاركة في ألواح الرسائل وهكذا. وعندما يبدأ هذا العنوان باستقبال أعداد كبيرة من السبام، يمكنك أن تلغيه وتوقف بذلك ورود السبام إلى هذا العنوان. يمكنك أن تسأل مزود الخدمة ISP أو مزود بريد الوب الذي تتعامل معه لتعرف فيما إذا كان يقدم ميزة مشابهة.

لا تشترِ شيئاً من مرسلي السبام

لو التزم كل شخص في العالم بهذه الخطوة، لانتهى وجود السبام. ولكن لسوء الحظ يوجد في هذا العالم عدد كاف من الناس الساذجين لكي يشتروا أشياء تم الإعلان عنها عن طريق السبام. وهكذا سوف تعتمد على الحلول التقنية حتى يأتي اليوم الذي يُعالج فيه هذا الغباء.

أرسل تقريراً بالسبام والتصيد

يمكنك أن ترسل تقارير برسائل السبام والتصيد إلى مختلف المؤسسات بما في ذلك مزود الخدمة، الحكومة، والمؤسسات المضادة للسبام والمضادة للتصيد. عندما ترسل تقـــارير عـــن السبام، تساعد مزود الخدمة على ضبط إمكانيات كشف السبام لديه؛ فقد يقدم تقريرك دليلاً أوضح إذا كان المزود يقرر أن يتخذ إجراءً قانونياً بحق مرسل السبام. دقق مع مزود الخدمـــة الخطوات التي يفضلها من أجل إرسال تقارير السبام. يوجد خدمة مجانية تـــدعى SpamCop ترسل تقارير عن السبام وتضيف مصدر السبام إلى اللائحة المحجوزة. يجب أن تسجل في موقع الوب (www.spamcop.net) ويجب أن يكون مستضاف البريد الإلكتروني لديك قادراً على عرض كامل ترويسات الرسالة (ليس فقط الترويستين :To و:From). انظـــر إلى الأســـئلة المتكررة FAQ في برمجيات بريدك الإلكتروني لتعرف المزيد عن عرض الترويسات كاملة.

ويمكنك أن ترسل تقارير عن رسائل السبام والتصيد أيضاً إلى لجنة التجارة الفيدراليـــة FTC. فهذه اللجنة تجمع رسائل السبام لكي تستخدمها في ملاحقة مرسلي السبام قانونيـــاً. يمكنك أن تبعث رسائل السبام إلى spam@uce.gov (UCE اختصار للبريـــد الإلكتـــروني التجاري غير المطلوب، مصطلح مهذب عن السبام).

وأخيراً، يمكنك أن تبعث رسائل التصيد إلى مجموعة العمل المضادة لرســـائل التصـــيد APWG. تفضل هذه المجموعة أن لا يرسل الناس رسائل التصيد. بدلاً من ذلك، افتح رسالة جديدة واكتب في العنوان reportphishing@antiphishing.org، والصق رسالة التصيد في الرسالة الجديدة وأرسلها.

6-6 الأدوات المضادة للسبام

إن الحرب ضد السبام تقودها تقنياً مزودات الخدمة ومدراء الشركات وملقمات البريد الإلكتروني الشخصية بشكل رئيسي. وبشكل عام تكون هذه الحرب بدون علم المستخدمين (إلا عندما تجد رسالة سبام قد وجدت طريقها إلى صندوق بريدك). تسمح معظم مـــزودات الخدمة للمستخدمين بدرجة محددة من التخصيص. على سبيل المثال، تسمح الخدمـــة AOL للمشتركين بإنشاء لوائحهم السوداء ولوائحهم البيضاء، استخدام ترشيح الكلمة الأساســـية، وحجز الصور الموجودة في الرسائل الواردة من المرسلين غير المعـــروفين. وتســـمح الخدمـــة Yahoo! للمستخدمين بإنشاء لوائح سوداء وحجز الصور ومرشدات الوب. أمـــا الخدمـــة Earthlink فتسمح للمستخدمين بحجز أي بريد من المرسلين غير الموجودين في دليل العناوين الشخصي (الشكل الأقصى من اللوائح البيضاء).

تتوفر أيضاً برمجيات للمستخدمين الذين يرغبون بتطبيق مستوى إضافي مـــن الـــتحكم

بالسبام من كمبيوتراهم المنـــزلية. يفصّل الجدول 6-1 بعض الخيارات. ويمكن أن تســتخدم محرك بحث على الوب وتكتب في حقل البحث "anti-spam software" أو "spam filters" فتحصل على عدد من الخيارات المهمة. وتتوفر أيضاً بحلات الكمبيوتر وتقارير على الوب عن المنتجات المضادة للسبام مـــن PC Magazine (www.pcmagazine.com)، PC World (www.pcworld.com)، وCNET (www.cnet.com). كانت الأسعار تتراوح في منتصف 2005 من 29.95$ إلى 39.95$ للبرمجيات المضادة للسبام المستقلة. ومن 49.95 إلى 79.95$ للمجموعات الأمنية التي تضم البرمجيات المضادة للسبام مع برمجيات أساسية أخـــرى تضـــم البرمجيات المضادة للفيروسات، البرمجيات المضادة للسبايوير، وجدار النار. لاحظ أن العروض الخاصة والمساومات تؤثر على السعر النهائي.

الجدول (6-1):

منتجات مختارة مضادة للسبام			
المنتج	**البائع**	**موقع الوب**	**المزايا**
Anti-Spam Personal	Kaspersky Lab	www.kaspersky.com	غير متوفر عند طباعة الكتاب. يعرّف السبام بالاعتماد على آراء أكثر من مليون مستخدم. من أجل أوتلوك وأوتلوك إكسبريس.
Cloudmark SafetyBar 4.0	Cloudmark	www.cloudmark.com	اللوائح السوداء، اللوائح البيضاء، كشف الخداع ورسائل التصيد، خيارات التحدي والاستجابة. من أجل أوتلوك وأوتلوك إكسبريس، هات ميل وMSN.
Norton AntiSpam	Symantec	www.symantec.com	اللوائح السوداء، اللوائح البيضاء (يتزامن مع دليل

منتجات مختارة مضادة للسبام			
المنتج	البائع	موقع الوب	المزايا
			عناوين أوتلوك، أوتلوك إكسبريس وإيدورا)، يرشح السبام من خدمة البريد Yahoo!Web، ويمكنه حجز البريد الإلكتروني في اللغات الأجنبية.
OnlyMyEmail Personal	OnlyMyEmail	www.onlymyemail.com	يعتمد على الخدمة. محركات تحليل متعددة، لوائح سوداء، لوائح بيضاء. من أجل أوتلوك، أوتلوك إكسبريس وبريد الوب.
Panda Platinum Internet Security 2005	Panda Software	www.pandasoftware.com	محرك تحليل، لوائح بيضاء، كشف رسائل التصيد. من أجل أوتلوك وأوتلوك إكسبريس.
PC-cillin Internet Security	Trend Micro	www.trendmicro.com	يمكنه أن يرشح السبام من أجل أوتلوك إكسبريس، AOL، Yahoo!، MSN، هات ميل وإيدورا.
Spam Filter Express	ANVSOFT	www.spam-filter-express.com	ترشيح بايسان، اللوائح السوداء، اللوائح البيضاء. من أجل أوتلوك وأوتلوك إكسبريس.

منتجات مختارة مضادة للسبام			
المنتج	البائع	موقع الوب	المزايا
SpamKiller	McAfee	www.mcafee.com	يتضمن اللوائح السوداء، اللوائح البيضاء، تواقيع السبام، ترشيح الصور، وترشيح اللغة الأجنبية.
ZoneAlarm Security Suite	Zone Labs	www.zonelabs.com	يوجه السبام إلى ثلاثة مجلدات: بريد تحت الاختبار، بريد تافه، بريد مخادع.

7-6 لائحة التدقيق

استخدم هذه اللائحة كدليل مرجعي للمواد المغطاة في هذا الفصل.

ما يجب أن تفعله

- حذف الرسائل المشبوهة بدون أن تفتحها.
- قراءة سياسات الخصوصية.
- عدم الكشف عن عنوان بريدك الإلكتروني قدر الإمكان.
- إرسال تقارير عن رسائل السبام والتصيد إلى FTC ومجموعة العمل المضادة لرسائل التصيد.

ما يجب أن لا تفعله

- نقر الارتباطات ضمن الرسائل التي تبدو بأنها مشبوهة.
- وضع عنوان بريدك الإلكتروني على الوب.
- شراء أي شيء من مرسل السبام.
- التأثر برسائل البريد الإلكترونية التنبيهية التي تطلب إجابة فورية.

8-6 موارد مساعدة

يقدم هذا القسم موارد إضافية لمساعدتك على تعلم المزيد.

Spamroll هي مجلة حول كل شيء عن السبام. تغطي الأخبار عن عالم السبام، تقدم معلومات عن رسائل السبام والتصيد، وتحتوي على أرشيف برسائل السبام. ويمكنك أن تساهم أيضـــاً في الأرشـــيف برســـائل الســـبام الـــتي وردت إليـــك. انظـــر إليـــه في الموقـــع www.spamroll.com.

يمكنك أن تستخدم SpamCop لمساعدتك على إرسال تقارير عن الســـبام إلى مـــزود الخدمة. ويقدم SpamCop أيضاً لائحة سوداء لمزودات الخدمة ومدراء البريد الإلكتروني. انظر إليه في الموقع www.spamcop.net.

يتعقب ديفيد سوركين تشريعات السبام في الولايـــات المتحـــدة والعـــالم، في الموقـــع www.spamlaws.com . ولكي تشاهد الرسوم CAN-SPAM وتشـــريعات المقترحـــات لجلسة الكونغرس الحاليـــة، اذهـــب إلى الموقـــع http://www.spamlaws.com/federal/index.shtml.

لكي تحصل على مزيد من المعلومات عن السبام، اذهب إلى موقع وب الســـبام للجنـــة FTC http://www.ftc.gov/bcp/conline/edcams/spam/index.html. ويمكنـــــك أن ترسل السبام أيضاً إلى spam@uce.gov، فتستخدمه اللجنة FTC لكي تلاحق مرسلي السبام قانونياً. ويحتوي موقع الوب أيضاً على توصيات حول منع السبام من الوصول إلى صـــندوق بريدك.

لكي تقرأ التقرير Pew Internet & American Life Project الكامل عـــن الســـبام اذهب إلى الموقع www.pewinternet.org/pdfs/PIP-Data-Memo-on-Spam.pdf.

تتعقب Abuse.net المعلومات حول مرسلي السبام والتقنيات المضادة للسبام. يوجد في الصفحة http://spam.abuse.net/userhelp/ العديد من الارتباطات المفيدة إلى توصـــيات وأدوات حول مواضيع مختلفة، بما في ذلك ترشيح وحجز رسائل السبام، إخفاء عنوان بريدك الإلكتروني، مصادر عناوين البريد الإلكتروني التي يمكن رميها، طريقة تعقب رسائل الســـبام، وطريقة إرسال التقارير حول السبام إلى مزود الخدمة.

الفصل السابع

تأمين ويندوز

تستخدم ملايين الكمبيوترات عبر العالم نظام تشغيل ويندوز وتطبيقات مايكروسوفت. وتوجد عدة نظريات تشرح أسباب سيطرة مايكروسوفت: التسويق الذكي؛ المبرمجون الجيدون؛ رغبة الشركة بتصريح برمجياتها إلى جميع مصنعي الكمبيوترات؛ إصرار أبل على التصرف بشكل معاكس، وبالتالي التخلي عن نصيب كبير من السوق إلى مايكروسوفت. مهما كانت الأسباب (وهناك بعض الحقيقة في كل منها)؛ فإن مايكروسوفت تملك أكبر نظام تشغيل ومجموعة تطبيقات سائدة على الأرض.

إن هيمنة مايكروسوفت هو أمر جيد لمجموعتين: حاملي أسهم مايكروسوفت والأشخاص الذين ينشئون برامج المالوير. عندما يسيطر نظام تشغيل واحد على السوق فإنه ينشئ بيئة خصبة للفيروسات، الديدان، أحصنة طروادة، والسبايوير. وجميع البرمجيات تعاني من نقاط خلل، ويمكن استغلال جميع أنظمة التشغيل ومنصات التطبيقات. ولكن عندما تسيطر عائلة من البرمجيات، فإن مبرمجي المالوير الذين يريدون الحصول على أكبر تأثير يسعون لتحقيق هدفهم. وقد يتم استبدال شعار ويندوز بسهولة بدائرة الهدف.

لقد أصبحت الإنترنت محرك للتجارة، لذلك فإن مهاجمة أكثر منصات عمل البرمجيات انتشاراً يحقق أفضل النتائج. لقد تم سؤال سارق مصارف مغمور، "لماذا تسرق المصارف؟" فأجاب "لأن النقود توجد في المصارف". وشيفرة مايكروسوفت هي المصرف الأكبر في العالم، لذلك فإنها تجذب كثيراً من انتباه الناس الذين يحاولون التسلق إليها من القبو إلى السقف، يكسرون النوافذ أو يدخلون ببساطة من الباب الأمامي مع بنادقهم. يأتي المجرمون مع مخططات عديدة، ومعظمها يدور حول استغلال نظام التشغيل ويندوز أو برنامج استعراض الوب إنترنت إكسبلورر (IE).

هل تتعرض مايكروسوفت حقاً للهجوم؟ أجرت USA Today[1] اختبار بيّن أنه خلال فترة أسبوعين، تم حصول 8177 محاولة في اليوم لاختراق كمبيوتر يشغل ويندوز XP سرفيس

باك 1 (SP1) على وصلة إنترنت DSL. إنه رقم كبير بشكل مدهش، وخصوصاً أن الاختبار لم يحصي عمليات الهجوم باستخدام وسيلتين أخريين: البريد الإلكتروني واستعراض الوب.

لكن تسعاً فقط من هذه المحاولات قد نجح، ولم يكن الكمبيوتر يستخدم أي برمجيات أمنية وتنقصه الرقع الأحدث. وبالمقابل، فإن كمبيوتر ويندوز XP يشغل جدار النار Zone Alarm، تعرض إلى 50 محاولة في اليوم، ولم ينجح أي منها. (شمل الاختبار أيضاً كمبيوترات تشغل Mac OS X وLinspire، نظام تشغيل يعتمد على لينوكس موجه للمستخدمين من مايكروتيل). لقد عانى الكمبيوتر OS X من عدد من محاولات هجوم مثل كمبيوتر ويندوز الذي يشغل SP1 (على الرغم من أن أياً منها لم ينجح). أما الكمبيوتر Linspire فقد تعرض إلى محاولات هجوم أقل بثمانمائة مرة، ولم ينجح أياً منها.

إن النصيحة الأسهل التي أعطيك إياها هي استخدام نظام تشغيل مختلف عندما تشتري كمبيوتر في المرة القادمة. يفاخر مناصرو أنظمة التشغيل بأن حماية ماكينتوش ولينوكس أسهل لأنها منتجات أفضل. إن الحكم على صحة هذا الأمر تتعدى قدراتي. ولكن يمكنني القول بأن معظم برامج المالوير تهاجم منصات مايكروسوفت، وعند استخدام نظام تشغيل بديل فسوف تتعرض لعمليات هجوم أقل.

إذا كنت تستخدم كمبيوتر ويندوز، يجب أن تقفله. الشيء الأول الذي تؤديه هو تثبيت جدار نار وإعداده على النمط الصامت. والشيء الثاني هو ضمان الحصول على الرقع الأحدث لنظام تشغيل ويندوز وجميع التطبيقات التي تستخدمها (بما في ذلك تطبيقات غير مايكروسوفت). وأخيراً، اتخذ الخطوات الضرورية لتأمين إنترنت إكسبلورر. يجب أن تجرب أيضاً استخدام برنامج استعراض مختلف، مثل Firefox أو Opera. على الرغم أنه يمكن قرصنة هذه البرامج، لكنها تتجنب بعض الأمور الأمنية المرتبطة مع IE وهي أهداف أصغر تلقى مقدار أقل من انتباه المجرمين (مع أن هذا الوضع يتغير بسرعة بالنسبة لبرنامج الاستعراض Firefox بسبب ازدياد انتشاره).

"يمكن اختراق الكمبيوترات غير المحمية في دقائق"، للكاتب بايرون أكويدو وجون شوارتز، USA Today، 29 تشرين الثاني، 2004.

يبحث هذا الفصل في محددات تأمين ويندوز XP سرفيس باك 2 (SP2). إن ويندوز XP SP2 هو الإصدار الأحدث من نظام تشغيل مايكروسوفت للمستخدمين وهو الذي تدعمه مايكروسوفت حالياً. وسوف نبحث أيضاً بتأمين IE بشكل أفضل وأين يمكن الحصول على برامج استعراض بديلة.

1-7 ويندوز XP سرفيس باك 2

إن مايكروسوفت على دراية تامة بأن منتجاتها تتعرض لهجوم متواصل، وأنها تتعرض

لتشويه سمعتها على المدى الطويل (إذا لم تتعرض أيضاً إلى انخفاض مبيعاتها) إذا استمر ويندوز بأن يكون علفاً لمبرمجي المالوير النهمين والمتدخلين الماكرين. إن ويندوز XP وسرفيس باك 2 يؤديان معزوفة واحدة من مايكروسوفت لكي تثبت قدرة منصة ويندوز الأمنية ولكي تعكس سمعتها بأنها طعم جيد. تتوفر الترقية SP2 مجاناً، بافتراض أنك قد اشتريت XP. وإذا كنت تستخدم إصدار أقدم من ويندوز، فيجب أن تشتري نظام تشغيل جديد، ويجب أن يتضمن SP2.

إذا كنت تشغل ويندوز XP، يمكنك أن تحمّل SP2 من Windows Update (لكنه ملف كبير، لذلك يجب أن تخصص بعض الوقت لتحميله) أو يمكن أن تطلب الترقية على قرص مضغوط في الموقع www.microsoft.com/windowsxp/sp2/default.mspx. يمكن أن يحصل مستخدمو ويندوز XP على القرص المضغوط مجاناً.

يبحث القسم التالي بما هو جديد في SP2 – على الأخص آليات الحماية المبينة في البرمجيات.

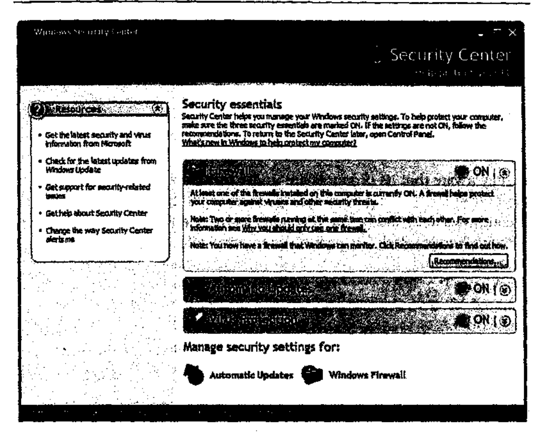
مركز أمن ويندوز

إن التحسين الرئيسي في SP2 هو مركز الأمن، الذي يجمع عدة تحكمات أمنية مهمة في مكان واحد. فمركز الأمن يسمح لك بمراقبة حالة البرمجيات المضادة للفيروسات (AV)، إدارة جدار نار ويندوز، وإعداد عمليات تحديث البرمجيات التلقائية.

لكي تصل إلى مركز الأمن، انقر على الزر Start ثم اختر Control Panel و Security Center (الرمز المدرع). عندما يفتح إطار مركز الأمن، ترى ثلاث لوحات رئيسية: Firewall جدار النار، Automatic Updates عمليات التحديث التلقائية و Virus Protection الحماية من الفيروسات (انظر إلى الشكل 7-1). ويوجد على كل لوحة حالة مضيئة للإشارة فيما إذا كانت الوظيفة مؤهلة. ويوجد على كل لوحة أيضاً زر يتحكم بشاشة منسدلة إلى الأسفل تقدم مزيد من المعلومات حول كل وظيفة.

يوجد تحت اللوحات رمزان: Automatic Update، وWindows Firewall. يمكنك أن تنقر على كل رمز لكي تنشط الوظائف وتغير الإعدادات. ويقدم الإطار Resources في الزاوية العليا اليسرى ارتباطات إلى معلومات أمن إضافية.

لنبدأ بالرمز Windows Firewall. يقدم ويندوز XP SP2 جدار نار أساسي يمنع الكمبيوترات الأخرى الموجودة على الإنترنت من الوصول إلى كمبيوترك ما لم تصل إليها أولاً. ويتم تأهيل عمل جدار نار ويندوز بشكل افتراضي، لذلك إذا كنت تستخدمه كجدار النار الوحيد، فإنه مؤهل افتراضياً.

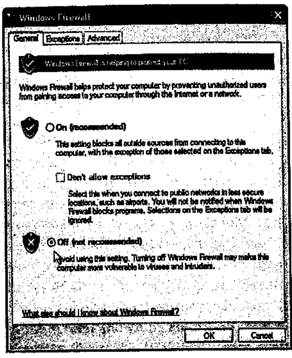


الشكل (7-1): مركز الأمن في ويندوز.

كما تم نقاشه في الفصل الثالث، "جدران النار"، على الرغم من أن جدار نار ويندوز يؤدي عملاً ممتازاً لمنع الوصلات غير المطلوبة التي تأتي من الإنترنت إلى كمبيوترك، ولكنه لا يؤدي شيئاً لمواجهة الديدان أو الفيروسات التي تصل إلى كمبيوترك وتحاول أن تقيم وصلات من كمبيوترك إلى الإنترنت. وهكذا يؤدي جدار نار ويندوز نصف العمل فقط (على الرغم أنه النصف الأهم). لكن جدار النار المناسب يجب أن يراقب محاولات الكمبيوتر لإقامة وصلات مع الإنترنت. وذلك لأن برامج المالوير والسبايوير تفتح غالباً وصلات الإنترنت لترسل تقريراً إلى ملقم التحكم، لتحصل على التعليمات المحدثة أو لتبدأ عمليات هجوم ضد أهداف جديدة. فجدار النار الذي يراقب الاتصالات الصادرة يمكن أن ينبهك إذا أراد برنامج مشبوه أن يتحدث بشكل مفاجئ إلى كمبيوتر على الإنترنت.

يذكر الفصل الثالث جدران نار عديدة تقدم كلتا الوظيفتين، ونوصي بأن تحصل على أحدها وتثبته على كمبيوترك. إذا كنت تستخدم جدار نار مختلف، تحتاج إلى إلغاء تأهيل جدار ويندوز أولاً. لن تكون محمياً بشكل مضاعف باستخدام جدار نار من شركة أخرى في الوقت نفسه مع جدار نار ويندوز. وبالفعل فإن تشغيل جداري نار أو أكثر على الكمبيوتر نفسه وفي الوقت نفسه يمكن أن يقاطع استخدام الإنترنت. لكي تلغي تأهيل جدار نار ويندوز،

انقر على الرمز Windows Firewall في أسفل صفحة مركز الأمن. فيفتح إطار منبثق، كما هو مبين في الشكل 7-2؛ انقر الزر Off. كما يمكن أن تلغي بعض جدران النار من الشركات الأخرى تاهيل جدار نار ويندوز خلال عملية التثبيت.



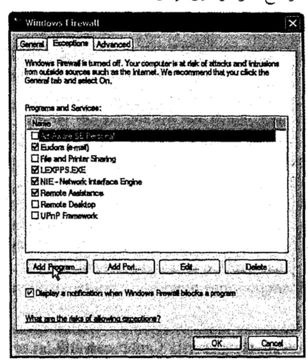
الشكل (2-7): صفحة جدار نار ويندوز.

حتى لو ألغيت تأهيل جدار نار ويندوز، فإن مركز الأمن يطلعك على وجود جدار نار من شركة أخرى وما إذا كان مؤهلاً. يجب أن تكون مايكروسوفت قادرة على البحث عن معظم جدران النار المعروفة جيداً.

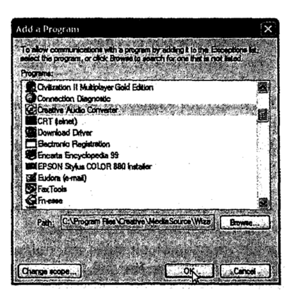
إعداد جدار نار ويندوز

إذا شغلت جدار نار ويندوز، يجب أن لا تزعج نفسك بإعداد المهام العامة مثل التجول على الوب وإرسال واستقبال البريد الإلكتروني. على كل حال، تحتاج إلى الإطلاع على بعض أمور الإعداد الأساسية. يمكن أن يمنع جدار النار بعض البرامج، مثل الألعاب أو برمجيات الرسائل الفورية، من أن تفتح وصلة إلى الإنترنت. يمكنك أن تغير هذا الإعداد بنقر الرمز Windows Firewall في أسفل صفحة مركز الأمن. فيظهر الإطار المبين في الشكل 7-2. انقر على علامة التبويب Exceptions، ترى لائحة بعنوان Programs and Services، كما هو مبين في الشكل 7-3. ابحث في هذه اللائحة عن البرنامج الذي تريد أن تسمح له بالاتصال مع الإنترنت لتعرف فيما إذا كان موجوداً. إذا لم يكن موجوداً، انقر الزر Add Program ثم

ابحث في اللائحة Programs، كما هو مبين في الشكل 7-4. حدد البرنامج وانقر OK. فيتم نقل البرنامج إلى اللائحة Programs and Services، كما هو مبين في الشكل 7-3. تأكد أن البرنامج الذي أضفته مدققاً، ثم انقر على الزر OK. فيسمح عندئذٍ جدار نار ويندوز لـذلك البرنامج بالوصول إلى الإنترنت.



الشكل (7-3): علامة التبويب Exceptions في جدار نار ويندوز.

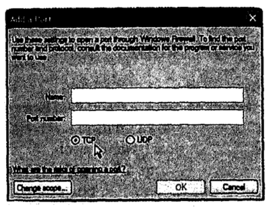


الشكل (7-4): مربع حوار إضافة برنامج.

يجب أن تبقي عدد الاستثناءات صغيراً قدر الإمكان. كلما ازداد عدد الاستثناءات التي تنشئها، تزداد الثقوب المقحمة في جدار النار، فيزيد احتمال أن ينجح المتـدخل أو برنـامج مالوير بالوصول إلى كمبيوترك.

يمكنك أن تضيف أيضاً منافذ إلى لائحة الاستثناءات. يسمح المنفذ في الكمبيوتر لبرامج أو خدمات معينة بالاتصال مع كمبيوترك. على سبيل المثال، تستخدم حركة مرور الوب المنفذ 80. ويعرف كمبيوترك أي المنافذ يحتاج لفتحها من أجل التطبيقات العامة مثـل الإنترنـت والبريد الإلكتروني. تستخدم بعض البرامج منافذ مختلفة (على سبيل المثال، ألعاب على الوب، المحادثة الهاتفية VoIP، والرسائل الفورية)، لذلك قد تحتاج لفتح هذه المنافذ يدوياً لكي تعمل البرامج. على كل حال، كما مع البرامج، كلما قل عدد المنافذ المفتوحة يقل عـدد الثقـوب الموجودة في جدار النار.

إذا عرفت المنفذ (أو المنافذ) التي تريد أن تفتحها، انقر الزر Add Port على الشاشة المبينة في الشكل 7-3. فيتم فتح إطار جديد يدعى Add a Port، كما هو مبين في الشكل 7-5. يسمح لك بإدخال اسم ورقم المنفذ.



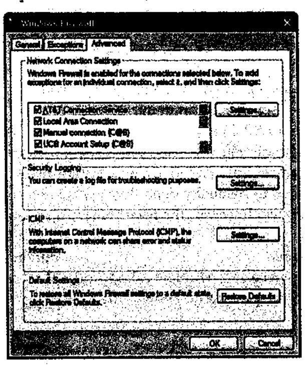
الشكل (7-5): مربع حوار إضافة منفذ.

يمكن أن تستخدم أيضاً علامة التبويب Advanced لمتابعة إعداد جدار النار، كما هـو مبين في الشكل 7-6. يوجد في هذا الإطار أربعة أقسام: Network Connection Settings إعدادات وصلة الشبكة، Security Logging تسجيل الأمن، ICMP، وDefault Setting الإعدادات الافتراضية.

يجب أن ترى تحت إعدادات وصلة الشبكة الوصلة المقامة إلى مزود الخدمة.

وتحت تسجيل الأمن يمكنك أن تنشئ سجل أمني لكي تـرى الوصـلات المسـموحة والممنوعة. لن تكون هذه السجلات مفيدة ما لم يكن لـديك بعـض الخـبرة في شـبكات الكمبيوتر، ولكن إذا كنت مهتماً برؤية شكل العناوين IP، المنافذ التي يستخدمها الكمبيوتر،

والعناوين IP للأماكن التي تتصل بها، يجب أن تلقي نظرة على السجل. (يمكن أن ترى عينـــة عن السجل في الشكل 3-2 في الفصل الثالث). يملك ويندوز SP2 XP ملف وجهة افتراضي للسجلات (C:WINDOWS/pfirewall)، ولكن يمكنك كتابة الملف في أي مكان تريـــده. لاحظ أن وظيفة السجل تعمل فقط من أجل جدار ويندوز. أما إذا كنت تستخدم جدار نار من شركة أخرى، فإنه ينشئ سجلاته الخاصة، والتي يجب أن تعثر عليها من واجهة المستخدم.



الشكل (7-6): علامة التبويب Advanced في جدار نار ويندوز.

يشمل تنسيق السجل تاريخ ووقت كل عملية، وصف للعملية (على سبيل المثال، لكي تفتح وصلة إلى كمبيوتر آخر)، البروتوكول (TCP وهكذا)، عناوين IP المصدر والوجهـــة، منافذ المصدر (أي كمبيوترك) والوجهة، ومعلومات عن الرزم المنفردة التي تشكل الاتصالات عبر الإنترنت. لمزيد من المعلومات عن المنافذ، البروتوكولات واتصالات الإنترنت، انظـــر إلى الفصل الثالث.

تسمح علامة التبويب Advanced في القسم ICMP للكمبيوتر بإرســـال واســـتقبال رسائل بروتوكول رسالة التحكم بالإنترنت (ICMP). وهذا البروتوكول مفيد لمدراء شبكات الكمبيوتر لكي يحصلوا على معلومات عن صحة النظام، لكن لا يحتاج مستخدمي الكمبيوتر للاهتمام برسائل ICMP. وبالفعل، فإن بعض المهاجمين يستخدمون الرسائل ICMP لكـــي يعرفوا طريقة استجابة الكمبيوتر. وهكذا، يفضل أن لا تؤهل الرسائل ICMP.

أخيراً، قسم الإعدادات الافتراضية هو نقطة البداية من جديد وهو مفيد إذا سببت كل هذه الإعدادات مشاكل مع التجول في الإنترنت. انقر Restore Defaults لكي تعيد جدار نار ويندوز إلى إعداداته الأصلية. لاحظ أن نقر الزر Restore Defaults يمسح أي تغيير أجريته على جدار النار، بما في ذلك البرامج التي سمحت بها، المنافذ التي فتحتها وهكذا.

الحماية من الفيروسات

لا يقدم ويندوز XP SP2 حماية من الفيروسات، لكنه يخبرك عن وجود برنامج AV من شركة أخرى وعما إذا كان البرنامج يملك التحديثات الأخيرة. على كل حال، لاحظ أن مايكروسوفت لا تراقب جميع البرمجيات AV. يمكنك أن تعرف ما إذا كانت برمجياتك AV مدعومة بالذهاب إلى الموقع www.microsoft.com/security/partners/antivirus.asp. تذكر لائحة جزئية من البرامج AV المدعومة Symantec، Trend Micro، Computer Associates، GFI، F-Secure، Sophos، Kaspersky، McAfee، وPanda Software.

لاحظ أنه مع أن مايكروسوفت لا تقدم برمجيات مضادة للفيروسات (على الرغم من أن ذلك سوف يتغير على الأغلب مع الإصدارات الجديدة من نظام تشغيل مايكروسوفت)، ولكنها تقدم أداة مجانية لتدقيق الكمبيوتر من أجل برامج المالوير. تمسح أداة إزالة البرمجيات الخبيثة Malicious Software Removal كمبيوترك من أجل لائحة من البرمجيات الخبيثة ثم تزيل أي مالوير تجده. عندما كنت أكتب هذا الفصل، كشفت الأداة 20 عائلة (بما في ذلك الإصدارات) من الديدان والفيروسات المعروفة. إذا كنت تستخدم برمجيات من شركة أخرى، فيجب أن تكوم محمياً من برامج المالوير المذكورة. على كل حال، إذا كان الفضول يعتريك فإنه لا يضيرك أن تحمّل الأداة وتجرب عملها. يمكنك أن تحمّل الأداة في www.microsoft.com/security/malwareremove. إذا أهّلت عمل Automatic Updates (انظر إلى القسم "تأهيل التحديثات التلقائية")، يتم تحميل الأداة وتشغيلها تلقائياً. وعندما تنتهي الأداة من العمل، تحذف نفسها. ولكن تذكر أن هذه الأداة ليست بديلاً عن برنامج متخصص مضاد للفيروسات. حتى ولو كانت تزيل النماذج العامة من برامج المالوير، فهي لا تمنع هذه البرامج من الوصول إلى كمبيوترك. وبالمقابل فإن برنامج حديث مضاد للفيروسات يمكنه أن يكشف ويحجز برامج المالوير قبل أن يثبت نفسه على الكمبيوتر. وبالإضافة إلى ذلك، فإن أداة إزالة البرمجيات الخبيثة تكشف وتزيل مجموعة محددة فقط من برامج المالوير والتي يمكن لمنتج مضاد للفيروسات أن يكشفها ويزيلها.

الحماية من طفح الدارئ

يساعدك SP2 على حماية نظام تشغيل ويندوز وعدة بروتوكولات اتصالات من تقنية هجوم تدعى طفح الدارئ. باستخدام هذه التقنية، يحاول برنامج خبيث أن يحقن شيفرة زائدة،

تفوق طاقة الكمبيوتر على التعامل معها، في منطقة من ذاكرة الكمبيوتر (تـدعى الـدارئ). تحتوي هذه الشيفرة على تعليمات للتحكم بالكمبيوتر، وتنساب إلى منطقة أخرى من الذاكرة ويتم تنفيذها. تعتمد الديدان المؤتمتة بشكل خاص على طفح الدارئ. تتأثر معظم أنظمة تشغيل وتطبيقات الكمبيوتر بطفح الدارئ. وفي حين أن SP2 لا ينهي تهديد طفح الـدارئ، لكنـه يحسّن مقاومة ويندوز.

2-7 ثلاثاء الرقع

تتطلب جميع البرمجيات عملاً دؤوباً بشكل دائم؛ ولا توجد نقطة حيث ينتهي العمل في البرمجيات. في بعض الأحيان يكون ذلك لأن باعة البرمجيات يصدرون الإصدار التـالي مـن البرمجيات الذي يعزز المزايا والوظائف الجديدة. على كل حال، يصدر باعة البرمجيات رقعـاً جديدة بين الإصدارات المحددة. وهذه الرقع هي كتل برمجية تصحح المشـاكل الموجـودة في البرنامج. بعض هذه المشاكل هي علل وظيفية تتداخل مع التشغيل الطبيعي للبرنـامج. علـى سبيل المثال، قد تسبب علة البرمجيات أن تعرض حاسبة الكمبيوتر نتيجة العملية 2+2 بأنها 5.

كما توجد فئة خاصة من العلل أيضاً تدعى نقاط الخلل. يمكن أن يستغل شخص آخر نقطة الخلل في البرمجيات من أجل الوصول إلى الكمبيوتر وتنفيذ عملاً ما. والعديد من الديدان التي تجوب الإنترنت هي أمثلة عن برامج المالوير المصممة لاستغلال نقاط خلل البرمجيات. في بعض الأحيان، يتم كشف نقاط الخلل من الشركة التي أنشأت البرمجيات. ولكن غالبـاً مـا يكتشفها باحث من خارج الشركة. فالعديد من الشركات تجد رزقها بالبحث عن نقاط الخلل في البرمجيات. والشركات الثلاثة الأكثر شهرة هي Secunia، eEye وX-Force (وهي ذراع البحث لشركة أمن تدعى Internet Security Systems). تحصل هذه المؤسسات البحثيـة على دعاية لبراعتها في كشف نقاط الخلل، وهكذا، تحاول مثل الصحف الإخبارية أن تسـبق بعضها البعض، يحاول هؤلاء الباحثون أن يسبقوا منافسيهم دوماً.

عندما تكتشف مؤسسة بحث نظامية خللاً برمجياً، فإن البروتوكول المقبول هو الاتصال ببائع البرمجيات المصابة. توافق مؤسسات البحث عادةً على إعطاء البائع فترة زمنية (لنقل 40 يوماً، لكن هذه الفترة تتغير بشكل كبير) لكي يتأكد من نقطة الخلل الموجودة ولينشئ رقعة. وعندما تصبح الرقعة جاهزة، يعلن الباحث والمؤسسة على العمـوم نقطـة الخلـل فـيمكن للمستخدمين والمؤسسات أن تحمّل هذه الرقعة.

لسوء الحظ، لا يحترم الجميع مثل هذا البروتوكول. فقد يكتشف الباحثون المغمـورون نقاط خلل ولا يخبرون بائع البرمجيات المصابة. بل يبقون المعلومات عن نقاط الخلل لأنفسـهم لكي يستغلوها أو يبيعوها إلى الآخرين. وفي بعض الحالات يعلنون عن نقـاط الخلـل علـى العموم، فيعرف بها البائع والمهاجمون في الوقت نفسه. وفي هذه الحالة، يبدأ السباق بين البائع

الذي يحاول إنشاء رقعة والمهاجمين الذين يحاولون استغلال نقطة الخلل.

ولكي يبدو الأمر في حالة أسوأ، يصدر المجرمون أداة هجوم بسرعة كبيرة. على سبيل المثال، أعلنت مايكروسوفت في تشرين الأول 2000 عن رقعة لنقطة خلل في برمجيات ملقمها. وبعد عام تقريباً ظهرت الدودة Nimda، والتي هاجمت نقطة الخلل. وبالمقابل، أعلنت مايكروسوفت في نيسان 2004 عن رقعة إضافية لبرمجيات ملقمها؛ وبعد 17 يوماً قفزت الدودة Sasser إلى الساحة.

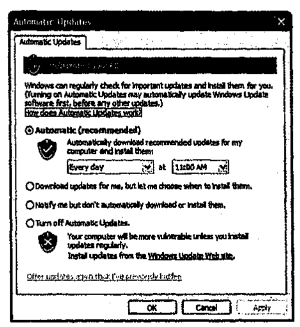
المشكلة الأخرى مع الرقع هي أن المستخدمين لا يثبتوها بعد إصدارها. على الرغم من أن الرقعة كانت متوفرة لمدة 336 يوماً قبل ظهور الدودة Nimda، لم يثبت عدد كافٍ من المستخدمين الرقعة فوجدت الدودة Nimda جميع ما احتاجت إليه من كمبيوترات تحتوي على الخلل المنشود لكي تنتشر بشكل واسع.

لقد كانت مايكروسوفت تعلن عن الرقع بشكل عشوائي. ولكن مع ازدياد عدد نقط الخلل، قررت الشركة أن تستخدم جدول رقع دوري. تعلن مايكروسوفت الآن عن تحديثات البرمجيات المؤخرة في كل ثاني ثلاثاء من كل شهر. وتركّز مايكروسوفت على الرقع التي تغطي نقاط الخلل المهمة، وهي النقاط التي تعطي المهاجم البعيد تحكماً كاملاً بالكمبيوتر أو تسبب أذىً كبير. تضم رقع الثلاثاء عادةً نقطة خلل مهمة واحدة على الأقل لكل رقعة. وبالطبع تصدر مايكروسوفت رقع طوارئ خارج الجدول المقرر إذا كانت نقطة الخلل خطرة.

يقدم ويندوز XP SP2 إمكانية التحديث التلقائي. فيمكنك أن تعدّ كمبيوترك لكي يتصل بموقع وب مايكروسوفت بأوقات دورية ويدقق الرقع الجديدة. ويوصى المستخدمين المنزليين على الخصوص بتأهيل ميزة التحديثات التلقائية لأنه، كما ذكرنا، يمكن أن يصدر المهاجمون أدوات هجوم خلال أيام أو أسابيع من الإعلان عن نقطة الخلل. لذلك بتحديث النظام بشكل تلقائي، تحظى بالحماية الفورية من عمليات الهجوم المتوقعة. والفائدة الأخرى هي أنك لا تحتاج لتذكر أن تزور مايكروسوفت كل شهر وتحصل على الرقع الأحدث. أخيراً، إن الخدمة التلقائية مريحة، لأنها تهتم بالرقع لعدد كبير من منتجات مايكروسوفت، بما في ذلك نظام تشغيل ويندوز، إنترنت إكسبلورر، والتطبيقات الشائعة. وهكذا، إذا لم يتم تغطية نقطة خلل جديدة في ويندوز ميديا بلير، على سبيل المثال، لا تحتاج إلى الذهاب إلى موقع آخر لكي تحصل على الرقعة.

تأهيل التحديثات التلقائية

لكي تؤهل التحديثات التلقائية، انقر على الرمز Automatic Updates في أسفل شاشة مركز الأمن، كما هو مبين في الشكل 7-1. فيفتح ذلك إطار أصغر يدعى Automatic Updates، يسمح باختيار الإعدادات (انظر إلى الشكل 7-7).



الشكل (7-7): مربع حوار التحديثات التلقائية.

يمكنك أن تختار تحميل وتثبيت التحديثات تلقائياً (هذا هو الإعداد الموصـــى بـــه مـــن مايكروسوفت) أو يمكنك أن تختار التكرار والوقت الذي تحصل فيه عملية التحـــديث. وإذا اخترت وقتاً يكون فيه كمبيوترك مغلقاً، فإن عملية التحديث تتم في المرة التالية عندما تعيـــد تشغيل كمبيوترك. ولكي تبقى على بر الأمان، أوصي باختيار وقتاً يكون كمبيوترك موصولاً إلى الإنترنت لكي تضمن استقبال عملية التحديث.

يمكنك أن تختار أيضاً تحميل التحديثات تلقائياً ولكن أن يتم تثبيتها عندما تطلب ذلك أو يمكنك أن تطلب تنبيهك بتوفر عمليات التحديث بدون أن يتم تحميلها أو تثبيتـــها تلقائيـــاً، ويمكنك أيضاً إلغاء تأهيل التحديثات التلقائية.

يمكـــن أن تـــدقق أنـــك حصـــلت علـــى جميـــع التحـــديثات بالـــذهاب إلى http://windowsupdate.microsoft.com. (يجب أن تستخدم إنترنت إكسبلورر الإصدار 5 أو الأحدث لكي تصل إلى هذا الموقع – لن يعمل مع Firefox). وبعد أن تصل إلى الموقع، تقدم مايكروسوفت خيارين: Express Install تثبيت سريع، الذي يحمّل التحديثات الأمنية والتحديثات المهمة، وCustom Install تثبيت مخصص، الذي يسمح باختيار عمليات تحديث محددة من اللائحة.

3-7 تأمين إنترنت إكسبلورر

كما أن ويندوز هو نظام التشغيل الأوسع انتشاراً في العالم، فإن إنترنت إكسبلورر هـــو

برنامج استعراض الإنترنت الأكثر استخداماً. ويسبب ذلك مشكلة مألوفة: يزيد الأشخاص السيئون من فرصهم في التحكم بكمبيوترك أو تثبيت البرمجيات بدون إذنك عن طريق مهاجمة برنامج الاستعراض الأكثر استخداماً.

أمن إنترنت إكسبلورر

يمكن أن يتعامل المهاجمون مع إنترنت إكسبلورر بطرق متعددة. وإحدى الطرق بالاستفادة من نقاط خلل البرمجيات. على سبيل المثال، ظهر في حزيران 2004 حصان طروادة يدعى Download.ject. وقد استغل خللاً برمجياً في ملقم معلومات إنترنت (IIS، ملقم الوب لمايكروسوفت) وإنترنت إكسبلورر. لقد تم تحميل الشيفرة الخبيثة أولاً على ملقمات وب تعاني من خلل. ثم تم تحميل مسجل ضربات المفاتيح لحصان طروادة خلسة إلى كمبيوترات المستخدمين الذين تجولوا إلى موقع الوب المصاب باستخدام إنترنت إكسبلورر. إن Download.ject هو مثال عن التحميل بالتجول.

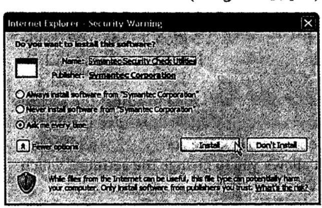
هناك أسلوب آخر وهو استخدام برنامج الاستعراض كمركبة لتحميل الشيفرة الخبيثة. يستطيع المهاجمون إما أن يخدعوا المستخدم بتحميل البرمجيات (باستخدام الهندسة الاجتماعية) أو يجبروا برنامج الاستعراض على تحميل البرمجيات بدون علم المستخدم بالاستفادة من الإعدادات الأمنية المنخفضة. تعتمد برامج السبايوير والأدوير غالباً على برنامج الاستعراض لكي يصلوا إلى كمبيوتر المستخدم.

التعامل مع أكتيف إكس

إن أحد أسباب كون استعراض الوب وسيلة شائعة لنقل برامج السبايوير والمالوير هو التقنية أكتيف إكس. وهي تقنية من مايكروسوفت تجعل صفحات الوب أكثر جاذبية – على سبيل المثال، باستخدام التحريك أو بالقدرة على فتح تطبيقات أخرى في برنامج الاستعراض (مثل مايكروسوفت وورد أو أدوبي). وبالإضافة إلى تحريك صفحات الوب، يمكن للتقنية أكتيف إكس أن تنفذ أيضاً برامج، تدعى تحكمات أكتيف إكس، على كمبيوترك عبر إنترنت إكسبلورر. تتعامل تحكمات أكتيف إكس مع نظام التشغيل كأي برمجيات تنفيذية أخرى. إن بعض تحكمات أكتيف إكس غير مؤذية وتحسن من عملية الاستعراض، لكن مبرمجي المالوير يكتبون تحكمات إكس أيضاً لتثبيت البرامج غير المرغوبة على كمبيوترك.

تدقق أكتيف إكس التوقيع الرقمي المرتبط مع جزء من البرمجيات الذي يجب تحميله. فالتوقيع الرقمي يضمن هوية المبرمجين. وفي حين أن التوقيع الرقمي لا يضمن كون البرنامج الفعلي آمناً، لكنه يساعد على تحديد البرامج التي تحاول التنكر كنوع آخر من البرمجيات. ويوصى أن لا تقبل بأي برمجيات مع توقيع رقمي غير مقبول.

يمكنك أن تضبط إعدادات برنامج الاستعراض IE بحيث يفتح إطار لكي يحــذرك عندما تتم محاولة تحميل أكتيف إكس ويعطيك الخيار بتثبيت البرنامج المحمّل أو عدم تثبيته (انظر إلى الشكل 7-8).



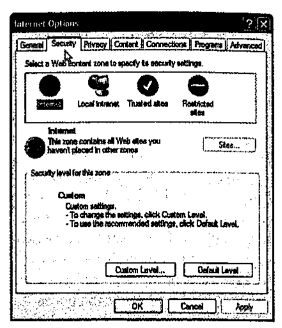
الشكل (7-8): تحذير أمني في إنترنت إكسبلورر.

لكي تدقق الإعداد، افتح IE واختر Tools ثم Internet Options. فيفتح إطار خيــار الإنترنت.

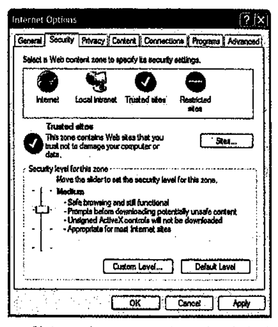
انقر على علامة التبويب Security، كما هو مبين في الشكل 7-9. ترى أربعة منــاطق وب يمكنك أن تضبط الإعدادات الأمنية من أجلها: Internet الإنترنــت، Local intranet الإنترانت المحلية، Trusted sites المواقع الموثوقة، وRestricted sites المواقع المحظورة. فكل منطقة تملك إعداداتها الأمنية التي يتم تطبيقها على أي موقع وب تضيفه إلى المنطقة. ويحصل أي موقع وب غير مذكور بصراحة في المنطقة على الإعدادات الأمنية لمنطقة الإنترنت. (لا تحتاج إلى تنفيذ أي شيء مع إعداد الإنترانت المحلية، فهو من أجل كمبيوترات ويندوز التي تشــكل جزء من شبكة الشركة).

لكي تضيف مواقع الوب إلى منطقة المواقع الموثوقة والمواقع المحظورة، انقر على المنطقــة التي تريد أن تضيف الموقع إليها وانقر على الزر ...Sites. اكتب في مربع الحوار الجديد عنوان الوب لكل موقع تريد أن تضمه إلى المنطقة.

يمكنك عندئذ أن تغير الإعدادات الأمنية لكل منطقة لكي تضبط التعليمات والإعدادات المرتبطة مع كل موقع وب تضمه إلى المنطقة. لكي تغير إعدادات كل منطقة، انقر على رمــز المنطقة التي تريد أن تضبطها. يجب أن ترى شريط زالقة يسمح بتغيير الإعدادات، التي تتراوح من Low إلى High (انظر إلى الشكل 7-10).



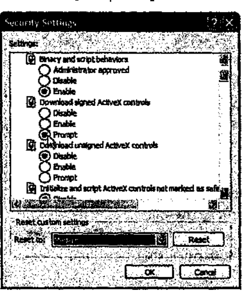
الشكل (7-9): علامة التبويب Security في مربع حوار خيارات إنترنت.



الشكل (7-10): ضبط إعدادات المواقع الموثوقة.

يمكنك أن تغير أيضاً المزايا الأمنية المنفردة بنقر الزر ...Custom Level. فيفتح مربع حوار الإعدادات الأمنية، كما هو مبين في الشكل 7-11. ويمكنك هنا إعداد القواعد المنفردة للتعامل مع تحكمات أكتيف إكس ووظائف برنامج الاستعراض الأخرى. على سبيل المثال، من أجل مواقع الوب في المنطقة الموثوقة، يمكنك أن تحدد الخيار Enable for the Download

signed Active controls فتسمح بتحميل تحكمات أكتيف إكس الموقعة بدون إعلامــك. ومن أجل المواقع الموجودة في منطقة الإنترنت يمكنك اختيار أن يطلب من الكمبيوتر الإذن قبل تحميل تحكمات أكتيف إكس الموقعة. أما من أجل منطقة المواقع الموثوقة، فيمكنــك اختيــار Disable وبالتالي لا يتم تحميل تحكمات أكتيف إكس.



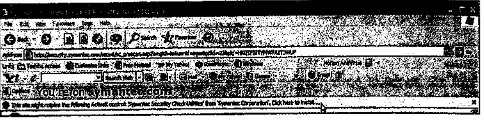
الشكل (7-11): تخصيص الإعدادات الأمنية.

إن تعديل الإعدادات المنفردة ضمن إطار الإعدادات الأمنية قد يــؤثر علــى طريقــة الاستعراض. يمكنك أن تختار أحد الخيارات (High، Medium، Medium-Low أو Low) في منطقة الإعدادات المخصصة Reset إذا أردت أن تعدل الإعدادات المنفردة. أو إذا عدلت هذه الإعدادات وأصبحت متداخلة يمكنك أن تنقر على الزر Reset كما هو مبين في الشكل 7-11. فيتم إعادة ضبط التغييرات إلى إعدادات مايكروسوفت الافتراضية.

لاحظ أنه طالما تضع الإعداد الأمني IE على Medium فإنك تتلقى رسائل تحذير؛ وأي إعداد أقل منه يسمح بتحميل تحكمات أكتيف إكس بدون إعلامك. ويوصى أن تختار الإعداد Medium على الأقل من أجل المنطقة الموثوقة. أما من أجل منطقة الإنترنت، فاختار الإعداد High أولاً وأرى مدى مقاطعته لعملية الاستعراض. تذكر أنه يمكنك دوماً وضــع المواقــع الموثوقة في المنطقة الموثوقة مع إعداد أخفض. على كل حال، لا أختار عادة أي إعداد أقل من Medium لمنطقة الإنترنت. ومن الواضح أنه يجب عليك اختيار الإعداد High من المنطقــة المحظورة (أو على الأقل لا تتجول إلى المواقع التي تضعها في المنطقة المحظورة).

يضيف ويندوز XP SP2 شريط أدوات (يدعى شريط المعلومات) إلى إنترنت إكسبلورر يظهر عندما يحتاج تحكم أكتيف إكس موقع إلى التحميل (انظر إلى الشكل 7-12). ويظهــر

شريط المعلومات تحت أي شريط أدوات آخر تضيفه إلى إنترنت إكسبلورر. عندما تنقر على شريط المعلومات، يعطيك الخيار بتحميل تحكم أكتيف إكس لتحصل على مزيد من المعلومات عن المخاطر الكبيرة التي تتعرض لها عند قبولك التحميل.



الشكل (7-12): شريط المعلومات.

إذا قبلت التحميل، يظهر مربع حوار لكي تؤكد على قبولك بتثبيت البرمجيات. وإذا كانت البرمجيات موقعة بشكل مناسب، يعرض مربع حوار اسم البرمجيات واسم ناشرها ويقدم ارتباطات إليهما للحصول على مزيد من المعلومات عنها (انظر إلى الشكل 7-8).

لسوء الحظ، حتى لو انبثق مربع حوار ينبهك عن تحكم أكتيف إكس غير متوقع، فإن النقر على No لا يساعد دائماً. يعامل بعض مبرمجو مالوير مربع الحوار بحيث يستمر تحميل البرمجيات حتى مع نقر No أو أي زر آخر. وقد يحاول المهاجمون أن يغيرون هذه الرسائل المنبثقة لكي تبدو كرسائل صادرة عن ويندوز أو كرسائل يولدها الموقع الذي تزوره. تكون هذه الرسائل عادة تحذيرية وتوجهك لتنفيذ عملية بشكل فوري، مثل النقر على الزر Yes لكي تشغل عملية مسح أو تحمّل برنامج لتصحيح المشكلة. يجب أن تتجاهل هذه الرسائل.

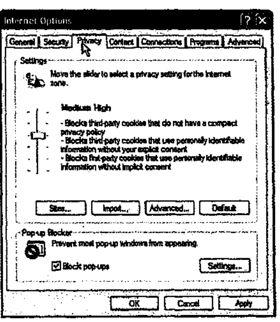
لكي تغلق مربعات الحوار والأطر المنبثقة بدون نقر الزر No أو Cancel أو المربع X في الزاوية العليا اليمنى، يمكنك أن تضغط F4+alt. فيغلق ذلك الأطر الموجودة ضمن برنامج الاستعراض بدون السماح بتنفيذ عملية التحميل.

إعداد الخصوصية

يقدم إطار خيارات الإنترنت خيارات أخرى بالإضافة إلى علامة تبويب الأمن من أجل التعديلات على إنترنت إكسبلورر، بما في ذلك General عام (حيث يمكنك إعداد صفحة البدء، حفظ ملفات الإنترنت المؤقتة، وإعداد سجل الصفحات التي زرتها) وPrivacy الخصوصية. يبحث هذا القسم بمزيد من التفصيل في إعدادات الخصوصية.

تسمح إعدادات الخصوصية بالتحكم بطريقة حفظ الكعكات المخزنة على كمبيوترك (انظر إلى الشكل 7-13). والكعكة هي ملف صغير تحفظه مواقع الوب على محرك القرص الصلب في كمبيوترك لتخصيص جلسة استعراض الوب. على سبيل المثال، تساعد الكعكات

مواقع التجارة الإلكترونية على تذكر أفضليات مستخدميها. يجب أن يـتم الحـديث عـن الكعكات في سياسة الخصوصية لموقع الوب. تفصّل سياسـة الخصوصـية طريقـة تجميـع المعلومات عن المستخدمين ومشاركتها من قبل موقع الوب. وبشكل عام، الكعكـات غـير مؤذية نسبياً.



الشكل (13-7): تعديل إعدادات الكعكات في IE.

على كل حال، تتعقب بعض الكعكات سلوكك عندما تتجول في الوب، وتسـجل في بعض الأحيان المعلومات الشخصية، مثل اسمك أو عنوانك. تستخدم هذه المعلومات في "بحث السوق" للمساعدة بتقديم الإعلان الموجّه. يتم تحميل كعكات أخرى في محرك القرص الصلب بدون أي تغطية في سياسة الخصوصية.

يضم إعداد الخصوصية شريط زالقة لإعداد طريقة تعامل برنـامج الاسـتعراض مـع الكعكات. تتراوح الإعدادات من قبول جميع الكعكات إلى حجز جميع الكعكـات. وبزلـق الشريط نحو الأعلى والأسفل، يمكنك أن ترى كيف يتعامل كل إعداد مع الكعكات المعروضة من المواقع التي تزورها والكعكات من المصادر الأخرى. تعرّف مايكروسوفت الكعكات من المصادر الأخرى بأنها التي لا تصدر من الميدان نفسه الذي ينتمي إليه الموقع الـذي تـزوره. الكعكات من المصادر الأخرى تكون غالباً كعكات تعقب. أقترح أن تستخدم الإعداد High أو Medium-High.

يمكنك أن تنشئ سياسات لمواقع وب محددة. انقر على الزر ...Site لكي تضيف المواقع إلى لائحة تقبل بشكل دائم أو تمنع بشكل دائم الكعكات. يمكنك أن تغطي أيضاً إعـدادات شريط الزالقة بالنقر على الزر ...Advanced.

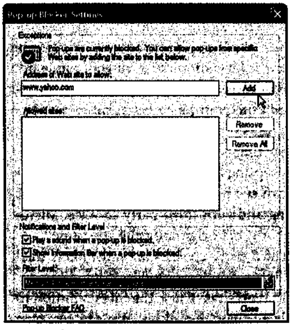
لاحظ أن مواقع الوب تعتمد بشكل كبير على الكعكات لجعل عملية الاستعراض أسهل. إذا اخترت أن تحجز جميع الكعكات أو أن يتم توجيهك لقبول الكعكات، فسوف تمضي وقتاً طويلاً بنقر Accept أو Deny عندما تزور مواقع الوب.

حاجز الأطر المنبثقة

تولد العديد من مواقع الوب إعلانات منبثقة عند زيارتك للموقع. تفتح الإعلانات المنبثقة أطر جديدة في مقدمة الصفحة التي تستعرضها. (ويتم عرض بعضها تحت الصفحة، وتراها بعد أن تغلق برنامج الاستعراض. تدعى بالأطر المنبثقة خلفياً). هذه الإعلانات مزعجة وخطرة لأن السبايوير والأدوير تستخدم الأطر المنبثقة كطريقة لخداعك وتثبيت برامجها.

يسمح إنترنت إكسبلورر 6.0 الذي يعمل على ويندوز SP2 بإغلاق هذه البرامج باستخدام حاجز الأطر المنبثقة. وهو مؤهل بشكل افتراضي، لكن يمكنك تخصيصه وإلغاء تأهيله إذا أردت ذلك.

لكي تؤهل (أو تلغي تأهيل) حاجز الأطر المنبثقة، انقر على علامة تبويب الخصوصية في إطار خيارات الإنترنت. ترى مربع تدقيق حجز الأطر المنبثقة في أسفل مربع الحوار (انظر إلى الشكل 7-13). لكي تبدأ عملية الإعداد، انقر Settings فيسمح لك مربع حوار إعدادات حاجز الأطر المنبثقة، المبين في الشكل 7-14، باستثناء مواقع محددة من وظيفة الحجز. يمكنك أن تحدد أيضاً طريقة إعلامك إذا تم حجز إطار منبثق.



الشكل (7-14): مربع حوار إعدادات حاجز الأطر المنبثقة.

بعدئذ، يمكنك إعداد مستوى المرشح على Low، Medium أو High. يسمح الإعداد Low بعرض الأطر المنبثقة من المواقع المحمية (أي المواقع التي تستخدم HTTPS، مثل موقع وب مصرفك). ويحجز الإعداد Medium معظم الأطر المنبثقة، ما عدا الأطر التي تأتي من مواقع وب ذكرتها في المنطقة الموثوقة. أما الإعداد High فيجب أن يحجز جميع الأطر المنبثقة. أوصي باستخدام الإعداد Medium أو High.

يمكنك أيضاً أن تحمّل أدوات مجانية تحجز الأطر المنبثقة. على سبيل المثال، يقدم كل من Yahoo! وGoogle أشرطة أدوات برنامج الاستعراض يمكنها أن تحجز الأطر المنبثقة. اذهب إلى http://toolbar.yahoo.com أو http://toolbar.google.com. تتوفر أشرطة الأدوات لبرامج الاستعراض الأخرى أيضاً.

4-7 برامج الاستعراض البديلة

إن الطريقة الأفضل لكي تمنع معظم عمليات الهجوم هي بالابتعاد عن أهدافها السائدة. كما ذكرنا، تحتوي جميع البرمجيات على نقاط خلل ويمكن مهاجمتها، لكن برنامج الاستعراض إنترنت إكسبلورر من مايكروسوفت هو الهدف المختار للمهاجمين. وبرامج استعراض الوب البديلة مثل Firefox وOpera تقع على مسافة بعيدة من حيث اهتمام المهاجمين بها بعد مايكروسوفت. وهكذا فإن الميزة الكبيرة لهذه البرامج هي أن تجذب انتباه مجرمي الإنترنت بنسبة أقل بكثير. وتقدم العناصر الأساسية مثل حجز الأطر المنبثقة، كما تقدم أيضاً مزايا أفضل من إنترنت إكسبلورر، مثل الاستعراض المبوب، والذي يدعك تحمل عدة أطر في برنامج استعراض واحد.

بالإضافة إلى معدل انتشارها غير الكبير، فهناك سبب آخر لكون هذه البرامج أكثر أمناً وهو أنها لا تستخدم أكتيف إكس. بدلاً من ذلك تستخدم تقنية تدعى جافا أبلت. ومثل أكتيف إكس، تستطيع جافا أبلت أن تحسن عملية الاستعراض وتساعد على تحميل البرمجيات. ولكن على العكس من أكتيف إكس، فإن جافا أبلت غير متكاملة مع نظام تشغيل الكمبيوتر، الأمر الذي يجعل من الصعب على المالوير أن تحصل على موطئ قدم. تعمل برامج جافا أبلت ضمن ما يدعى علبة الرمل، التي تعزل الأبلت وتمنحه الوصول إلى عدد محدود فقط من موارد الكمبيوتر الموجودة ضمن علبة الرمل. يمكن طبعاً استغلال وإساءة استخدام جافا أبلت، لكنها تقدم بشكل عام مستوى أكبر من الحماية.

أي أن هذه البرامج ليست وسيلة حماية سحرية ضد المهاجمين. وإذا اخترت برنامجاً بديلاً فإن القاعدة الأمنية "الحفاظ على البرمجيات محدثة" تظل صحيحة تماماً. يجب أن تحصل على أفضل الحلول الأمنية والرقع الحديثة لنقاط الخلل المكتشفة لوحدك - لا يعمل نظام تحديث ويندوز التلقائي مع منتجات أخرى ليست من مايكروسوفت.

لسخرية القدر، فإن العديد من هذه الحلول أصبحت شائعة (قام ملايين المستخدمين بتحميل برنامج الاستعراض Firefox)، وهي تجذب الآن انتباه عدد أكبر من المجرمين. سوف يتم اكتشاف عدد أكبر من نقاط الخلل، وسوف يتم استغلالها بعمليات هجوم جديدة. وفي النهاية سوف تفقد الميزة التي أدت إلى اختيارها.

هناك سيئة أخرى وهي أنه تم تصميم العديد من مواقع الوب بشكل متوافق مع إنترنت إكسبلورر، فبرنامج الاستعراض البديل قد يواجه مشاكل بتشكيل موقع الوب وجميع وظائفه. على سبيل المثل، لم أستطع استخدام Firefox لكي أطلب كتاباً من Amazon؛ واضطررت لاستخدام IE لكي أنهي المعاملة. على كل حال، لا توجد قاعدة تنص بعدم استخدام برامج استعراض متعددة على كمبيوترك. فالعديد من المستخدمين يستخدم برنامج استعراض بديل من أجل التجول في الوب ويستخدمون IE عند الضرورة.

تبحث الأقسام التالية في برنامجي الاستعراض Firefox وOpera كبديلين لإنترنت إكسبلورر واسعي الإنتشار.

(www.mozilla.org) Firefox

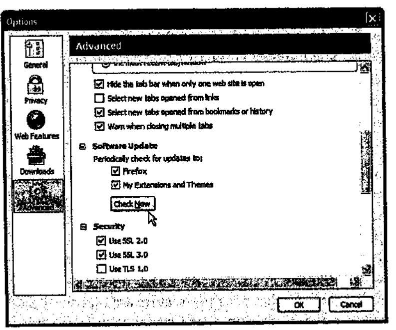
برنامج الاستعراض البديل الأكثر انتشاراً هو Firefox ويمكن تحميله مجاناً. يعتمد Firefox على برمجيات المصدر المفتوح؛ ويعني ذلك أن أي شخص يريده يمكن أن يحصل على نسخة من شيفرة المصدر، وهي المجموعة الأساسية من التعليمات البرمجية التي تخبر التطبيق أو البرنامج كيف يعمل. ويرحب بالمستخدمين الذين يحاولون التدقيق في شيفرة المصدر والعثور على نقاط الخلل، اقتراح التحسينات، وإضافة مزايا ووظائف جديدة يتم تعميمها على بقية المستخدمين. تتوفر معظم برمجيات المصدر المفتوح مجاناً ويتم خدمتها من قبل المتطوعين.

تقابل البرمجيات المملوكة برمجيات المصدر المفتوح. وتحرص الشركة مالكة البرمجيات على شيفرة المصدر. وتقوم الشركة بإنشاء مزايا، وظائف، وحلول لنقاط جديدة الخلل، حسب جدول الشركة.

إحدى فوائد برمجيات المصدر المفتوح هي أنها تستخدم الكثير من البرامج المضافة، ويمكن أن يعمل عليها العديد من الناس في الوقت نفسه. يمكن أن ترى هذه البرامج المضافة (التي تدعوها Mozilla بالملحقات) في الموقع /http://addons.mozilla.org.

كما ذكرنا، فإن Firefox ليس خالياً من المشاكل. بل هو عرضة لنقاط الخلل، ويجب أن تبقى متتبعاً لاكتشافها. لكي ترى لائحة بنقاط الخلل في برنامج الاستعراض، اذهب إلى www.mozilla.org/projects/security/known-vulnerabilities.html. تسرد هذه الصفحة نقاط الخلل التي تم معالجتها في كل إصدار جديد من برمجيات Firefox. وتسند أيضاً معدل أهمية لكل نقطة خلل.

لكي تجد الإصدار الأحدث من Firefox، بما في ذلك الحلــول الأمنيــة، اذهــب إلى www.mozilla.org/security. وإذا كنت تســتخدم Firefox وتريــد أن تبحــث عــن التحديثات الجديدة، اختر Tools ثم Options، فيفتح مربع حوار، انقر فيه Advanced. ترى مربع الحوار المبين في الشكل 7-15. مرر إلى أسفل الشاشة حتى ترى الإدخــال Software Update. إذا دققت المربعــات :Periodically check for updates to، فــإن برنــامج الاستعراض سوف يدقق موقع وب Firefox كل يوم من أجل التحديثات الجديدة. لاحظ أن Firefox لا يثبت هذه التحديثات تلقائياً – بل يوجهك قبل تثبيت أي برمجيات. عندما تنقر على Check Now، يدقق Firefox من أجل الإصدارات الجديدة من البرمجيات تلقائياً.



الشكل (7-15): تدقيق تحديثات البرمجيات Firefox.

Opera (www.opera.com)

يتوفر برنامج الاستعراض Opera بإصدارين: الأول مجاني، والآخر يكلف 39$. يولــد الإصدار المجاني إعلانات. عندما تثبت الإصدار المجاني من Opera يمكنك أن تختار بين استقبال الإعلانات الموجهة من Google أو الإعلانات السائبة. إذا اخترت الإعلانات الموجهــة مــن Google، يتم إرسال العنوان IP لكمبيوترك والمحددات URL الــتي تزورهــا إلى Google للمساعدة بتوليد الإعلانات التي تطابق أفضليات استعراضك. يحاول Google أيضاً أن يحدد موقعك الجغرافي بالاعتماد على العنوان IP للمساعدة بتوجيه الإعلانات. يدّعي Opera بأنه لا يجمــع المعلومــات الشخصــية. يمكنــك أن تجــد المزيــد مــن المعلومــات في www.opera.com/adsupport/ وفي www.opera.com/privacy.

لقد جربت إصدار الإعلانات السائبة. فخصص برنامج الاستعراض منطقة صـــغيرة في الزاوية العليا اليمنى من الصفحة للملصقات الدعائية؛ إنها ليس إعلانات مقتحمة ويمكن تحملها. وإذا أعجبك برنامج الاستعراض Opera ولكنك لا تحتمل الإعلانات، يمكنك أن تدفع 39$ وتتخلص من جميع هذه الإعلانات.

5-7 التدقيقات الأمنية

يجب أن تعدّ جدار النار وتختار تحكمات إنترنت إكسبلورر، ولكن يجب أن تدقق عملك أيضاً. يوجد في الإنترنت العديد من الموارد لتدقيق حالة الكمبيوتر الأمنية. والطـــرق الثلاثـــة التالية تستحق التدقيق بها.

(www.grc.com) ShieldsUp!

خدمة مجانية لتدقيق الإعدادات الأمنية لجدران النار الشخصية، بما في ذلك جدار نـــار ويندوز المبيت في SP2. كما ذكرنا في الفصل الثالث، تم تشغيل !ShieldsUp من قبل الخبير الأمني ستيف جيبسون لسنوات. يقدم الموقع عدة اختبارات، بما في ذلك اختبارين مناســـبين لجدار نار ويندوز. يدعى الأول، المنافذ العامة، يدقق 26 منفذ مستخدم بكثرة يمكن أن تكون مفتوحة (وبالتالي يمكن للأشخاص السيئين الوصول إليها). والاختبار الثاني، منافذ الخدمـــة، يدقق 1056 منفذاً، وهو اختبار شامل ويحتاج تنفيذه إلى وقت أطول. في كلتا الحالتين تكون النتائج واضحة وسهلة الفهم وتعطي فكرة عما إذا كان جدار النار يقوم بعمله. يقدم الموقـــع أيضاً ارتباطات لمزيد من المعلومات عن جدران النار الشخصية وأمن الكمبيوتر.

لكي تشغل الاختبارات، اذهب إلى www.grc.com ومرر إلى الأسفل إلى الارتبـــاط !Shieldsup. وباستخدام الخدمة فإنك تمـــنح الإذن الرسمـــي لـــلأداة !Shieldsup بمســـح كمبيوترك. يخبرك !ShieldsUp عن العنوان IP للكمبيوتر المستخدم لمسح كمبيوترك، فـــإذا كنت مهتماً يمكنك أن تراقب سجلات جدار النار بعد أن تشغل المسح لكي ترى كيف تبدو عملية المسح من جدار النار الذي تستخدمه.

(www.pivx.com/preview) PivX Preview

أداة أمنية مجانية من شركة تدعى PivX. تعطي الأداة كمبيوترك درجة أمنية وفق أربع فئـــات: Threat center مركـــز تهديـــد، Security software برمجيـــات آمنـــة، Patches/Hotfixes رقع وحلول برمجية، وFirewall Protection حماية جدار النار. يحلـــل PreView كمبيوترك ليحسب الدرجة الأمنية وفق هذه الفئات الأربعة. إنها طريقة بســـيطة لتوصيف نقاط الخلل الموجودة في كمبيوترك. على كل حال، يعتمد جزء مهم من الدرجة على استخدامك لمنتجات Pivx الأخرى، لذلك يجب أن نأخذ ذلك بعين الاعتبار.

(www.symantec.com/securitycheck) Symantec Security Check

تمسح هذه الأداة كمبيوترك من أجل مختلف نقاط الخلل المهمة، بما في ذلك المنافذ التي قد تستجيب للطلبات غير المطلوبة، وجود أحصنة طروادة، وفيما إذا كنت تشغّل برمجيات مضادة للفيروسات. كما أن نتائج الاختبار مفهومة، وتتوفر النتائج التفصيلية من أجل Hacker Test (الذي يبين المنافذ التي تستجيب والتي لا تستجيب لطلبات الوصلة). يحتاج الاختبار إلى تحميل أكتيف إكس لكي يعمل.

6-7 إنترنت إكسبلورر 7-0 وويندوز فيستا

تخطط مايكروسوفت لترقية إنترنت إكسبلورر ونظام تشغيل ويندوز. وسوف يكــون إنترنت إكسبلورر 7.0 متوفراً على الأغلب في خريف 2005. وعلى الرغم من أن التفاصيــل كانت قليلة عند كتابة هذا الكتاب، فقد وعدت مايكروسوفت بأن IE 7.0 سوف يضم دعماً أمنياً وأدوات جديدة لتحسين عملية الاستعراض. لقد توقع العديد من المراقبــون أن تقلــع مايكروسوفت عن إصدار نسخة جديدة من IE حتى تصدر الشركة نظام التشغيل الجديــد. على كل حال، أعلنت مايكروسوفت عن تاريخ إصدارها الجديد بعد أن شــهدت النهضــة الكبيرة لبرامج الاستعراض البديلة مثل Firefox. (فإنترنت إكسبلورر ما يزال يملك 90 بالمائة تقريباً من جميع برامج الاستعراض المستخدمة، لذلك ما يزال الطريق متاحاً لإقصاء Firefox).

يتوقع إصدار ويندوز فيستا (دعيت سابقاً لونغهورن)، نظام التشغيل الجديد، في أواخر خريف 2006. مرة أخرى، التفاصيل قليلة لكن مايكروسوفت وعدت بإضافة تحسينات أمنية جديدة بالإضافة إلى أداة رسوم، نظام حفظ ملفات جديد، والقدرة على تشــغيل إنترنــت إكسبلورر في منطقة معادية لجعل الأمر أصعب على مالوير أن تستخدم برنامج الاســتعراض كنقطة دخول إلى الكمبيوتر.

7-7 لائحة التدقيق

استخدم هذه اللائحة كدليل مرجعي للمواد المغطاة في هذا الفصل.

ما يجب أن تفعله

- تأهيل التحديثات التلقائية Automatic Updates لكي تضمن أن برمجيات مايكروسوفت مجهزة بالرقع الأمنية والحلول البرمجية الأحدث.
- الاستفادة من القدرات الأمنية في مركز أمن ويندوز، بما في ذلك مراقبة البرمجيات المضادة للفيروسات وجدار النار.
- استخدام جدار نار ويندوز إذا لم يكن جدار نار من شركة أخرى.

- استخدام برنامج استعراض وب بديل للتجول في الإنترنت.
- اتخاذ خطوات لضمان أن إنترنت إكسبلورر بخيرك قبل أن يبدأ بتثبيت تحكمات أكتيف إكس.

ما يجب أن لا تفعله

- عدم تحديث ويندوز إنترنت إكسبلورر.
- قبول تحكمات أكتيف إكس غير الموقعة.
- عدم تحديث برامج الاستعراض البديلة مع الحلول البرمجية الأحدث.
- تشغيل جداري نار أو أكثر على الكمبيوتر نفسه في الوقت ذاته.

7-8 موارد مساعدة

يقدم هذا القسم موارد إضافية لمساعدتك على تعلم المزيد.

تملك مايكروسوفت مختلف المعلومات الأمنية للمستخدمين وهي مكان جيد للبدء بتعلم التقنيات الأمنية الأساسية. اذهب إلى www.microsoft.com/athome/security لتتعلم المزيد عن تأمين ويندوز وتطبيقات مايكروسوفت.

يوجد منتدى للمستخدمين CastleCops من أجل مختلف المواضيع حول الكمبيوترات، بما في ذلك الأمن. يمكنك أن تنضم إلى hgمنتدى لكي تطرح أسئلة، تقرأ الرسائل المطروحة، وتحصل على المعلومات المساعدة حول أي شيء يتعلق بالكمبيوترات. وبالتحديد، إذا تجولت إلى http://castlecops.com/forums، يمكنك أن تمرر إلى أسفل اللائحة لكي تجد منتديات حول برامج الاستعراض (بما في ذلك أمن برنامج الاستعراض) وأنظمة التشغيل (بما في ذلك ويندوز وأمن ويندوز).

تتعقب مؤسسة البحث الأمنية Secunia نقاط الخلل الأمنية التي تم تزويد رقع من أجلها أو لم يتم تأمين هذه الرقع، في ويندوز وعدد من برامج الاستعراض الشائعة بما في ذلك إنترنت إكسبلورر وFirefox. المواد المكتوبة هي تقنية في طبيعتها لكن الموقع هو مكان جيد للبحث عن نقاط الخلل الأحدث التي قد تؤثر على الكمبيوتر. اذهب إلى www.secunia.com.



الفصل الثامن

المحافظة على أمن عائلتك على الوب

تشكل الإنترنت تحدياً كبيراً للآباء الحريصون. سواء كنت تحرص على منع المواد غير المقبولة كالصور الإباحية والعنف أو منع مستغلي الأطفال الذين يدخلون إلى غرف المحادثة، فإن الإنترنت تفتح عدداً غير منته من المداخل إلى مواقع الوب التي لا تريد أن تدخل إلى منزلك. على الجانب الآخر، قد يحتاج الآباء إلى حماية من أولادهم أيضاً. فصناعة الموسيقا والأفلام تتعامل مع اختراق حقوق النسخ بمنتهى الجدية هذه الأيام، وقد تجد نفسك متورطاً في قضايا قانونية أو استحقت عليك غرامات مالية لأن ولدك قام بتحميل الحلقة الثالثة من حرب النجوم أو حصل على أغنية بدون احترام حقوق النسخ.

تستفيد العديد من الشركات من ترشيح الوب وتحقق أرباح مرتفعة. وتحتوي منتجاتها على لوائح ضخمة بالمواقع التي قد لا تريد أن ينظر إليها موظفيها لأسباب تتعلق بالمسؤولية (يمكن أن تشكل الصور الإباحية في مكان العمل بيئة غير ودية وتنتهي بدعاوى قضائية) أو لأسباب إنتاجية (تشتت مواقع الرياضة، المقامرة والتجارة الإلكترونية انتباه الموظفين عن مهامهم). تستثمر الشركات أيضاً في التقنيات الضرورية لكشف وحجز برامج مشاركة الملفات ند إلى ند التي تسمح باختراق حقوق النسخ.

تتوفر العديد من الحلول التقنية للمنزل (مع أنها ليست شاملة وغير مضمونة بالتأكيد)، لكن يمكن أن يستفيد الآباء من الأدوات غير التقنية أيضاً، بما في ذلك الحدس العام وتنظيم الوقت.

يبحث هذا الفصل بالحلول الضرورية لحجب المواد غير المرغوبة من الوب. سوف نناقش العواقب القانونية والمالية لمشاركة الملفات وننظر إلى بعض أمور الأمن المرتبطة مع البرمجيات ند إلى ند. وسوف نناقش أيضاً أمور الأمن على الوب، مثل حماية أولادك من المستغلين على الوب. تتوفر حلول تقنية لبعض المشاكل المعروضة هنا أو على الأقل توجد أدوات لمساعدتك بحلها. لكن في معظم الحالات فإن الدفاع الأفضل هو أن تنمي إحساس عام بمضمون مواد

الإنترنت الجيدة لدى أولادك. تذكر أن الإنترنت كأي بيئة أخرى – لديها مناطق آمنة وأماكن خطرة، والنصيحة المعتادة حول عدم الحديث مع الغرباء تنطبق على الإنترنت أيضاً.

1-8 ترشيح المحتوى غير المرغوب

عندما كنت طفلاً كان هناك ثلاث طرق للحصول على مواد الكبار: البحث عن الأجزاء غير المحتشمة في الروايات المشهورة المتوفرة لدى والدي في المنــزل؛ تصفح المجلات النسائية الملقاة؛ ومشاهدة أفلام الكبار لساعات في بيت صديق يملك تقنية الكابل أملاً في مشاهدة منظر إباحي.

أما في هذه الأيام فالموقف مختلف بشكل كلي. الإنترنت هي المستودع الأكبر في العالم للبذاءة، ولا تحتاج إلا لبضعة استعلامات. يجب أن لا يشكل ذلك مفاجأة. فالمواد الإباحية عبرت على جميع وسائط الإعلام التي اخترعها الإنسان، بما في ذلك، الصور، المطبوعات، الأفلام، تلفزيون الكابل والفيديو المنــزلي. والوسط الوحيد الذي لا يحقق أرباحاً من المواد الإباحية هو الراديو (على الرغم من أن هاورد ستيرن يبدو أنه ينهي هذا الاستثناء). لا أعرف متى تم إرسال الصورة العادية الأولى من كمبيوتر إلى آخر عبر خط الهاتف، لكنني أراهن أنها تمت ضمن الأسبوع الأول من وصل الكمبيوترات.

والمواد الإباحية هي نوع واحد من مواد المحتوى السيئ: يوجد أيضاً العنف، مواقع الكره، القمار، غرف المحادثة وهكذا. ومما يضاعف المشكلة هو أن الإنترنت ينقصها العديد من المرشحات القائمة في أوساط أخرى. فمخزن الكتب لن يبيع مجلة إباحية لشخص عمره 11 عاماً، لكن موقع الوب سوف يسلم جميع مواد المحتوى السيئ وبأي كمية مطلوبة.

يملك الآباء مختلف الخيارات التقنية وغير التقنية في أيديهم. سوف نقترح بعض الأفكار لمراقبة نشاط أولادك على الوب ونشرح كيف تستخدم مرشحات برامج الاستعراض ومحركات البحث. على كل حال، هناك عدد كبير من الخيارات لتسليم المحتوى، والخيار الأقوى (بعد خيار فصل الإنترنت نهائياً) هو استخدام برمجيات مراقبة من شركة أخرى.

المراقبة الشخصية

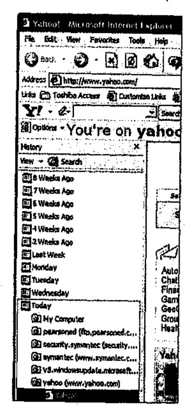
إن الترشيح الخشن هو أن لا تدع أولادك يصلون إلى الإنترنت في أماكن خاصة، مثل غرف نومهم. فإذا خصصت كمبيوتر في منطقة عامة مثل غرفة المعيشة لممارسة النشاطات على الوب، فستكون مؤثراً على هذه النشاطات. ومعرفة أن أي شخص يمر أمام الكمبيوتر قد يلمح ما هو معروض على الشاشة يقلل من محاولتهم للحصول على مواد المحتوى السيئ. قد يصعب تنفيذ ذلك في المنــزل حيث يحتاج أكثر من شخص للوصول إلى الإنترنت في الوقت نفسه أو إذا ثبت نقطة وصول لاسلكية تغطي المنــزل، ولكن القاعدة العائلية الجيدة هي "إذا كنت

موصولاً بالإنترنت، فأنت موجود في غرفة المعيشة أو على طاولة المطبخ" أو ما شابه.

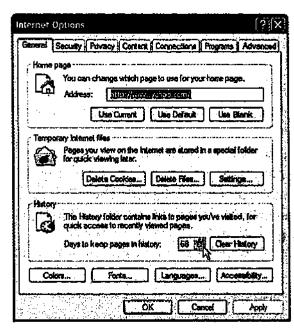
يمكنك أن تدقق ما يستعرضه أولادك على الوب بعرض سجلات المحفوظات History في برنامج استعراض الوب. يقدم كل برنامج استعراض منطقة يمكنك أن ترى فيها الصفحات التي تم زيارتها خلال فترة زمنية محددة، كأسبوع أو شهر. يمكنك أن تنقر المواقع المذكورة وتزور صفحات الوب الفعلية، وتدعك بعض برامج الاستعراض تبحث في سجلات المحفوظات لمواقع محددة. إن وظيفة المحفوظات مفيدة لتعقب المواقع التي تريد زيارتها مجدداً لكنك لا تتذكر العنوان بدقة. وهي مفيدة أيضاً لمراقبة نشاط أولادك على الإنترنت.

لكي تدقق المحفوظات في إنترنت إكسبلورر (IE)، كما هو مبين في الشكل 8-1، اختر View، Explorer Bar، History. وضمن سجل المحفوظات يمكنك أن تنقر View لكي تحصل على خيارات مختلفة لاستعراض السجل: حسب التاريخ، الموقع، تكرار الزيارة، وترتيب الزيارة.

لكي تعد عدد الأيام التي يتم تذكر الصفحات خلالها، حدد Tools، Internet Options. يظهر إطار صغير يقدم عدة أبواب في أعلاه. اختر علامة التبويب General، التي تعرض مربع صغير لإعداد المحفوظات (انظر إلى الشكل 8-2). يمكنك أن تحفظ سجلات من 0 إلى 999 يوم، لكن أسبوعين أو شهر تعتبر مدة كافية.



الشكل (8-1): عرض المحفوظات في إنترنت إكسبلورر.



الشكل (2-8): إعداد عدد الأيام التي يتم تذكر الصفحات خلالها.

إذا كنت تستخدم Firefox، يمكنك أن تعرض محفوظات الصفحة بالنقر على View، Sidebar، History. يظهر إطار يمتد على الجانب الأيسر من برنامج الاستعراض. كمـــا في إنترنت إكسبلورر، يمكنك أن تستخدم الزر View لكي تعرض المحفوظات حسب التـــاريخ، الموقع، تكرار الزيارة، وحسب الموقع الذي تم زيارته أخيراً. يمكنك أن تعـــد مـــدة ســـجل المحفوظات باختيار Tools، Options. في الإطار Options، انقر الرمز Privacy، فيفتح إطار داخلي يضم حقل إعداد المحفوظات.

يقدم الإطار المجاني لبرنامج الاستعراض Opera طريقة بسيطة للوصـــول إلى ســـجلات المواقع التي تم زيارتها، بما في ذلك رمز المحفوظات History في لوح على الجانب الأيسر مـــن برنامج الاستعراض. يمكنك أن تحدد أيضاً Tools، History. لكي تتحكم بالفترة الزمنيـــة لحفظ المواقع، حدد Tools، Preferences. عندما يفتح الإطار Preferences، انقر علـــى History قرب أسفل اللائحة على الجانب الأيسر من الإطـــار. وعلـــى العكـــس مـــن IE وFirefox، لا يحفظ Opera المواقع حسب التاريخ. بدلاً من ذلك، يمكنك أن تحـــدد عـــدد المواقع التي تحفظها، من 0 إلى 10000؛ وبعد بلوغ الحدّ الأقصى لعدد المواقع، يتم إلغاء المواقع القديمة عند إضافة مواقع جديدة.

قد تكون لاحظت أن جميع برامج الاستعراض تقدم الزر Clear History، كما هو مبين في الشكل 8-2. وبنقر هذا الزر يتم مسح سجلات المحفوظات الحالية. ومع أن تنفيذ هذا الأمر يمنعك من معرفة المواقع التي يزورها أولادك، فإن ذلك يشير أيضاً إلى أنهم ربما يزورون مواقع

لا يرغبون بأن تعرف عنها. وهكذا يجب احترام قاعدة عائلية وهي أنه لا أحد ينقر الزر Clear History.

لا تشعر بأنك مجبراً على القيام بتصرف مشين لمراقبة نشاطات التجول على الوب. وبالفعل، إذا أخبرت أطفالك أنك تراقب نشاطهم على الوب، فقد تساعد بإبعاد الأذى العابر الذي قد يتعرضون له.

ترشيح محرك البحث

يمكن إعداد محركات البحث الشائعة لكي ترشح المواد الجنسية الفاضحة من بحث الصورة والكلمة الأساسية. لا يحتاج ترشيح محرك البحث إلى برمجيات إضافية وهو سهل الإعداد. على كل حال، لا تضمن محركات البحث أن المواد غير المرغوبة لن تظهر في نتائج البحث. كما أن تأهيل المرشحات وإلغاء تأهيلها عملية سهلة. بالإضافة إلى ذلك، يجب أن تحفظ هذه الأفضليات في كل محرك بحث وفي كل برنامج استعراض وب تستخدمه. على سبيل المثال، إذا أعددت الترشيح الصارم Strict في Google باستخدام إنترنت إكسبلورر، لن يتم تطبيق هذا الإعداد على Google عندما تستخدم Firefox حتى تعد ذلك يدوياً. أخيراً، فإن محاولة إعداد كل محركات البحث المتوفرة على الإنترنت هو أمر غير مجدي.

فهل هناك سبب لتزعج نفسك بإعداد المرشحات؟ نعم. يضيف إعداد المرشحات على محركات البحث الرئيسية طبقة إضافية من الحماية ويخبر الشخص الذي يتجول على الوب بأن المواد الفاضحة غير مسموحة. ثانياً، قد يساعد الأطفال الصغار (الذين لا يحاولون الالتفاف على التعليمات الأبوية) على عدم عرض المواد الفاضحة بطريق الخطأ.

- يقدم ترشيح Google ثلاثة إعدادات: الترشيح الصارم Strict، الذي يزيل المواد الجنسية الفاضحة من عمليات البحث بالكلمة الأساسية والصورة؛ الترشيح المعتدل Moderate، الذي يرشح الصور الفاضحة فقط (هو الإعداد الافتراضي)؛ وبدون ترشيح No Filtering، الذي يفتح البوابة على مصراعيها. لكي تختار إعداداً، انقر على الارتباط Preferences على صفحة البدء Google، كما هو مبين في الشكل 8-3. فيفتح ذلك صفحة تسمح بضبط الإعدادات وتضم قسماً يدعى SafeSearch. مرر إلى الأسفل إلى المنطقة SafeSearch Filtering وحدد أحد الإعدادات، كما هو مبين في الشكل 8-4. يمكنك أن تحفظ عندئذ أفضلياتك، ولكن يمكن تغيير هذه الأفضليات من قبل أي شخص يستخدم برنامج الاستعراض.

Google

Web Images Groups News Froogle Local more »

Google Search | I'm Feeling Lucky

Advanced Search
Preferences
Language Tools

الشكل (8-3): ارتباط الأفضليات على صفحة البدء Google.

SafeSearch Filtering — Google's SafeSearch blocks web pages containing explicit sexual content from appearing in search results.
- Use strict filtering (Filter both explicit text and explicit images)
- Use moderate filtering (Filter explicit images only - default behavior)
- Do not filter my search results.

الشكل (8-4): المنطقة SafeSearch في Google.

- يقدم Yahoo! الترشيح SafeSearch مع ثلاثة إعدادات: ترشيح المواد الفاضحة من عمليات البحث عن الفيديو والصور على الوب؛ ترشيح عمليات البحث عن الفيديو والصور؛ وبدون ترشيح. انقر على الارتباط Advanced على صفحة البدء Yahoo! لكي تختار إعداداً، فتفتح صفحة البحث المتقدم على الوب. مرر إلى المنطقة SafeSearch Filter، حيث يمكنك أن تحدد أفضلياتك في الترشيح. لاحظ أن هذا الإعداد ينطبق على هذا البحث فقط. لكي تطبق إعداداتك على كل عمليات البحث، انقر الارتباط Preferences. فيفتح إطار جديد يدعى Search Preferences. يمكنك أن تضبط الإعداد لكل عملية ترشيح بحث ثم تحفظ الإعداد بالنقر على الزر Save Preferences في الزاوية العليا واليمنى. المشكلة مع هذا الإعداد هو إمكانية إلغاء تأهيله من أي شخص يستخدم الكمبيوتر.

يعطيك Yahoo! الخيار بإقفال أفضليات مرشح البحث، ولكن يجب أن تكون مستخدم ياهو مسجل. انقر على الارتباط Log In، اكتب في ياهو اسم المستخدم وكلمة المرور. اختر إعدادك، وانقر على مربع التدقيق لكي تقفل SafeSearch في النمط الذي اخترته. يمكنك عندئذ أن تنقر Save Preferences. على كل حال، كما يذكر ياهو على الموقع، أي شخص وقّع في الكمبيوتر بعمر 18 أو أكبر يمكنه اجتياز إعدادات ياهو بسهولة.

- تقدم MSN ثلاثة مستويات من الترشيح: الصارم Strict، الذي يرشح النصوص والصور الجنسية الفاضحة؛ المعتدل Moderat، الذي يرشح الصور الفاضحة؛ وغير مؤهل Off. اذهب إلى www.msn.com وانقر على الزر Search إلى جانب حقل البحث، فيفتح إطار جديد. انقر على الزر Settings لكي تختار مستوى الترشيح المطلوب. يمكنك أن تحفظ الإعداد، ولكن لا توجد طريقة لمنع أي شخص آخر يستخدم الكمبيوتر من تغييرها.

ترشيح إنترنت إكسبلورر

يمكنك أن تحصل على مستوى أقوى من الترشيح بالاستفادة من إمكانيات إنترنت إكسبلورر. يؤدي ذلك إلى تجنب الخوض في إدارة الإعدادات على عدد كبير من محركات البحث (على الرغم من أنني أوصي بإعداد المرشحات على محركات البحث الرئيسية بالإضافة إلى ضبط برنامج الاستعراض). على كل حال، لاحظ أن نظام الترشيح IE متعب عند الإعداد والصيانة، وأن نظام التصنيف يعاني من نقاط خلل.

يقدم IE نظام ترشيح في برنامج الاستعراض يدعى مرشد المواد Content Advisor، وهو يستخدم نظام تصنيف مبيت يدعى RSACi (المجلس الاستشاري للبرمجيات). على كل حال، وفق موقع الوب للمجلس RSACi، فإن نظام التصنيف المذكور غير صالح الآن وقد تم تسليمه إلى هيئة تصنيف مواد الإنترنت (ICRA). ويمكن أن يستخدم مرشد المواد أيضاً نظام التصنيف من مؤسسة تدعى SafeSurf. سوف نبحث عملية إعداد مرشد المواد لكي يعمل مع ICRA.

لقد طورت ICRA مصطلحات تصف المواضيع العامة الخمسة: المواد الجنسية والتعري، العنف، اللغة، وسائل المحادثة، والمقامرة والمخدرات. يكتب مشغلو موقع الوب أسئلة اختبار تصنف مواد موقع الوب باستخدام 45 وصف مقترن مع المواضيع الخمسة. على سبيل المثال، إذا احتوى موقع الوب على مواد تقع ضمن المواد الجنسية والتعري، يمكن أن يشير الموقع إلى وجود الأعضاء التناسلية الذكرية والأنثوية وإلى أعمال جنسية فاضحة. بالاعتماد على نتائج أسئلة الاختبار، تولد ICRA شيفرة يمكن أن يربطها مشغل موقع الوب مع الموقع. يدقق برنامج الاستعراض إنترنت إكسبلورر هذه الشيفرة ويسمح أو يمنع الوصول بالاعتماد على الإعدادات المختارة في مرشد المواد.

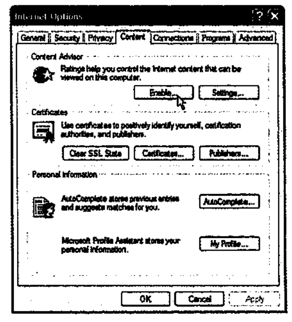
لاحظ أن ICRA لا تعمد إلى تسمية المواقع غير المقبولة؛ بل يتشارك مشغلو مواقع الوب بشكل طوعي في البرنامج ويكتبون أسئلة الاختبار بنفسهم. الخلل الواضح في هذا النظام هو أن ICRA لا تتخذ أي إجراء بحق المواقع غير المسماة. وأعتقد أن أغلبية مواقع التعري، العنف، والمقامرة على الإنترنت غير مسماة. (بتنفيذ اختبار سريع باستخدام نظام الاختبار في ICRA يتبين أن playboy.com يملك تسمية ICRA، لكن Penthouse.com لا يملك تسمية). بالإضافة إلى ذلك، يمكن الإجابة على أسئلة الاختبار بمعلومات غير صحيحة.

يستخدم SafeSurf نظام تصنيف مشابه من أجل تغطية مجموعة مشابهة من المواضيع، بما في ذلك مواضيع البالغين، المواضيع الجنسية، استخدام المخدرات والعنف. ومثل ICRA فإن Safesurf هو نظام طوعي لمزودات مواقع الوب.

لكي تستخدم نظام تصنيف ICRA ضمن مرشد المواد، يجب أن تحمّل أولاً ملف

التصـــنيف (يـــدعى rat. اختصـــاراً). يجـــب أن تحمّـــل هـــذا الملـــف مـــن الموقـــع www.icra.org/faq/contentadvisor/setup. حدد الخيار Save على شاشة التحميل. ثم احفظـــه علـــى كمبيـــوترك (إذا كنـــت تســـتخدم وينـــدوز XP) في الموقـــع C:\WINDOWS\System82. ويقدم موقع الوب المذكور دورة تعليميـــة جيـــدة لضـــبط إعدادات مرشد المواد بعد إضافة الملف rat. من ICRA.

حان الوقت الآن لإعداد مرشـــد المـــواد في إنترنـــت إكســـبلورر. حـــدد Tools، Internet Options. فيفتح إطار خيارات الإنترنت، كما هو مبين في الشكل 8-5. انقر علامة التبويب Content. ثم انقر Enable في القسم Content Advisor.



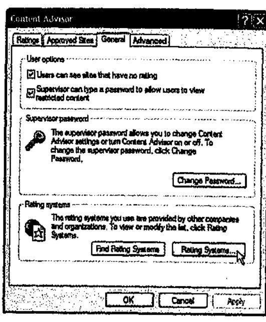
الشكل (8-5): علامة التبويب Content لمربع حوار خيارات الإنترنت.

عندما تعد مرشد المواد، يطلب منك أن تختار كلمة مرور. تجعلك هذه الكلمة المستخدم الرئيسي، فتتحكم بإعداد مرشد المواد، ويمكنك أن تسمح أو تمنع استعراض مواقع معينة. تأكد من اختيار كلمة مرور لن تنساها ولا يعرفها أولادك في الوقت نفسه.

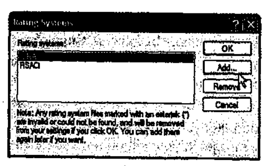
تقترح كل من مايكروسوفت وICRA بقوة أن تهتم بكلمة المرور بشكل كبير، لأنـــك إذا نسيتها، لن تكون قادراً على إلغاء تأهيل نظام ترشيح المواد، وقد ينتهي الأمر بمنع الوصول إلى المواقع التي تريدها. لا يملك أي من مايكروسوفت أو ICRA نسخة عن كلمـــة المـــرور، لذلك فهما غير قادرين على مساعدتك إذا أضعتها.

بعد أن اخترت كلمة مرور، تحتاج إلى اختيار الملـــف rat. ICRA. في مربـــع حـــوار خيارات إنترنت (المبين في الشكل 8-5)، انقر الزر Settings. فيفتح إطار جديد يدعى مرشد

المواد كما هو مبين في الشكل 8-6. انقر علامة التبويب General، ثم انقر ...Rating Systems فيفتح إطار صغير مع خيارات لإضافة وإزالة أنظمة التصنيف، كما هو مبين في الشكل 8-7. سوف يتم ذكر النظام RSACi على الأغلب ويجب أن تزيله لأنه لم يعد يعمل. ويجب أن تضيف الملف الذي حملته.



الشكل (8-6): علامة التبويب General لمربع حوار مرشد المواد.

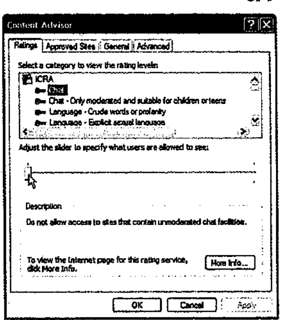


الشكل (8-7): مربع حوار أنظمة التصنيف.

لكي تضيف الملف ICRA، انقر الزر Add. فيفتح الملف system32، حيث حفظت الملف ICRA. انقر على الملف ICRA نقراً مزدوجاً. يجب أن تكون الآن ضمن مربع أنظمة التصنيف. حدد الخيار ICRA وانقر OK.

تابع الآن إلى علامة التبويب Rating في إطار مرشد المواد، كما هو مبين في الشكل 8-8. يجب أن ترى ICRA في اللائحة. يمكنك أن تضبط الإعدادات على عشرات الفئات، بما في ذلك المحادثة، اللغة، التعري وهكذا. إذا نقرت على فئة، يظهر شريط زالقة. يؤهل أحد

إعدادين: السماح للفئة المبينة أو منع الفئة المبينة. ويبدو أن الإعداد الافتراضي هو المنـــع. لا يدعم مرشد المواد بعض الفئات. ويطلب تصنيف ICRA أن تترك شريط الزالقة إلى أقصـــى اليمين.



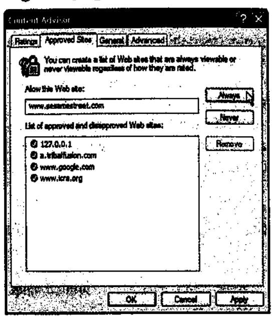
الشكل (8-8): علامة التبويب Ratings في مربع حوار مرشد المواد.

بعد أن تضبط الإعدادات، انقر Apply. يمكنك عندئذ أن تذهب إلى علامة التبويـــب General لكي تعد خيارات المستخدم الأساسية (انظر إلى الشكل 8-6). بما أن ICRA نظام تصنيف طوعي، فقد لا تشارك فيه مواقع الوب، ويعني ذلك عدم توفر درجـــات تصـــنيف. يمكنك إعداد مرشد المواد لكي تسمح للمستخدمين برؤية المواقع التي لا تملـــك تصـــنيفاً. أو يمكنك أن تعدها بحيث يحتاج المستخدم الرئيسي (أنت) إلى كتابـــة كلمـــة مـــرور ليـــدع المستخدمون يطلعون على المواقع غير المصنفة.

لقد اختبرت النظام لحجز جميع مواقع الوب التي لا تملك تصنيفاً. ومن بين المواقع التي تم حجزها بسبب عدم وجود تصنيف لهـــا كـــان: PBSKids.org، SesameStreet.com، ThomasTheTankEngine.com (نعم، لدي أطفال)، StarWares.com، ESPN.com، eBay.com، CNN.com وYahoo.com.

كما ترى، إذا حجزت جميع المواقع التي لا تملك تصنيفاً، فإنك تمنع كثيراً من المواقع غير المؤذية بالإضافة إلى المواقع التي تقدم المواد الفاضحة. على كل حال، إذا لم تحجز المواقع غـــير المصنفة، فإن اختبار موجز يبين أن العديد من مواقع المواد الإباحية غير مصنفة، لـــذلك فـــإن مرشد المواد يسمح باستعراض هذه المواقع إذا لم تعده على حجز جميع المواقع غير المصنفة.

ما الذي يجب أن تفعله؟ أحد الخيارات هو تحميل النظام بالمواقع الجيدة. يمكنك تنفيذ ذلك بفتح إطار مرشد المواد، النقر على Settings، ثم نقر علامة التبويب Approved Sites (انظر إلى الشكل 8-9). ويمكنك أن تكتب محددات URL للمواقع التي تسمح بها دائماً. (يمكنك أن تدخل أيضاً إلى المواقع التي لا تسمح بها أبداً).



الشكل (8-9): علامة التبويب Approved Sites في مربع حوار مرشد المواد.

وإذا حجزت أيضاً المواقع غير المصنفة، فإن المستخدم الرئيسي يملك الخيار بنقل المواقع المحظورة إلى لائحة المواقع المسموحة باستخدام كلمة مرور المستخدم الرئيسي. وفي كل مرة يحجز مرشد المواد موقعاً، يمكن أن يجري المستخدم الرئيسي ثلاثة تحديدات: السماح بعرض موقع الوب بشكل دائم، السماح بعرض صفحة الوب المحددة بشكل دائم أو السماح بالعرض خلال تلك الجلسة فقط. ويجب أن تدخل كلمة مرور المستخدم الرئيسي لكي تؤهل أي من هذه الخيارات.

وهكذا، إذا استخدمت ميزة تصنيف المواد، يجب أن تخصص الكثير من الوقت لوضع المواقع المسموحة في هذا القسم. كما يمكن أن تزعج عائلتك إذا اكتشفوا أن موقعاً غير مؤذ تم حجزه ولم تكن موجوداً لتلغي حجزه. إذا لم تمانع القيام بذلك، فإن مرشد المواد يقدم آلية ترشيح قوية جداً من أجل إنترنت إكسبلورر. على كل حال، إذا لم تكن مستعداً لتحميل المواقع المسموحة، ولا تفضل فكرة عدم حجز المواقع غير المصنفة، فإن مرشد المواد لن يكون مفيداً في مراقبة المواد غير المرغوبة.

ترشيح برنامج الاستعراض البديل

بحسب معلوماتي فإن برامج الاستعراض البديلة الشائعة، بما في ذلك Firefox وOpera (الإصدار المجاني)، لا تقدم أي آليات مبيتة لترشيح مواد الوب. لذلك، إذا كنت تستخدم أي من هذه البرامج على كمبيوترك، فيمكن أن يلتف أولادك بسهولة على مرشد المواد. على كل حال، تبني بيئة Firefox بشكل مستمر ملحقات لبرنامج الاستعراض. فعند كتابة هذا النص لم أستطع تحديد أي مشروع لترشيح مواد المواد غير المقبولة، لكن هذا الوضع قد يتغير. والشيء الأقرب الذي وجدته هو ملحق يدعى Image-Show-Hide. حسب هذا الوصف المختصر، فإن الملحق يسمح بعرض أو إخفاء جميع الصور على صفحات الوب. على كل حال، الآليـــة ببساطة هي زر بمكن تبديل حالته بين التأهيل أو عدم التأهيل، لذلك يسهل الالتفاف عليـــه. بالإضافة إلى ذلك، لا يرشح عملياً أي مواد غير مقبولة: إذا كان لديك، أهّله، فيخفي جميـــع الصور على كل صفحة وب تزورها، وهذا التصرف متطرف نوعاً ما. لكي تجد هذا الملحق، اذهب إلى http://addons.mozilla.org، انقر على ارتباط ملحقات Firefox، ثم انقر ارتباط استعراض الصور، الموجود في عمود على الجانب الأيسر من الصفحة. وقد تريد أيضاً أن تزور صفحة وب الملحقات ثم ترى فيما إذا تم كتابة ملحق الترشيح.

تحكمات مزود الخدمة

تقدم العديد من مزودات الخدمة آليات لحماية الأطفال على الوب وتقديم تجول آمن في الوب. الطريقة الأفضل هي بزيارة صفحة بدء مزود الخدمة أو الاتصال بقسم خدمة الزبائن. وفي غضون ذلك، إليك توضيحاً عن التحكم الأبوي المقدم من ثلاثة مزودات خدمة رئيسية. يجب أن تكون مشتركاً لتحصل فعلياً على هذه الخدمة.

- تقدم AOL عدد من مزايا التحكم الأبوي، بما في ذلك AOL Guardian، التي تبعـــث "بطاقة تقرير" بالبريد الإلكتروني إلى الآباء تبين فيها نشاطات البريد الإلكتروني، التجول والرسائل الفورية (IM). تضم المزايا الأخرى آلية توقيت للتحكم بفترة بقاء أولادك على الوب، قفل يمنعهم من تشغيل برامج الاستعراض البديلة، والقدرة على إنشـــاء لائحـــة بعناوين البريد الإلكتروني المقبولة. على كل حال، تعمل هذه المزايا إذا ســـجل أولادك الدخول بهوياتهم الفعلية. وأسهل طريقة للالتفاف حول هذه القيود هي باستخدام المحدد ID وكلمة المرور الخاصين بك. تقدم AOL الخدمة KOL أيضاً، والموجهة إلى الأطفال خصيصاً وتضم غرف المحادثة التي يتم مراقبتها من كادر AOL. يجب أن تشـــترك مـــع AOL للحصول على هذه الخدمة.
- تقدم Earthlink تحكم أبوي مجاني مع خيارات خدمة الاتصال الهاتفي والخدمـــة عاليـــة السرعة. وتقدم في أعلى القائمة ترشيح مواقع الوب. يمكنك إما أن تحـــدد اســـتعراض

أولادك بـ 15000 موقع تم قبولها من Earthlink أو تمنحهم الوصول الكامل إلى الإنترنت، ما عدا 3 ملايين موقع تحجزها Earthlink كجزء من نظام التحكم الأبوي. ويمكن أن تزيل Earthlink تلقائياً اللغة غير اللائقة من مواقع الوب. كما تقدم أيضاً وسيلة اتصال بسيطة للأطفال CyberFriends Communicator تضم البريد الإلكتروني، المحادثة، لوح المراسلة، والرسائل الفورية. فيمكن للآباء: إنشاء لائحة بيضاء بالأشخاص الذين يمكن لأولادهم الاتصال بهم. ويمكن أن يراجع الآباء جميع رسائل البريد الإلكتروني التي أرسلها واستقبلها أطفالهم باستخدام CyberFriends Communicator. أخيراً، يمكن أن يحدد الآباء الوقت الذي يقضيه أطفالهم على الوب. كما ذكرنا، يمكن تطبيق هذه التحكمات إذا كان أولادك يوقعون هويتهم فقط.

■ الخدمة Children's internet على الوب مخصصة للأطفال. فهي تجهز سطح المكتب فيستطيع الأطفال أن يستخدموا المزايا المبينة في الخدمة فقط (تضم استعراض الوب، البريد الإلكتروني والمحادثة). إذا كان ولدك يملك كمبيوتره الخاص، فقد تكون هذه الخدمة خياراً جيداً، انظر إلى www.childrensinternet.com لمزيد من المعلومات.

التحكم بالسبام

إن الكثير من البريد التافه هو إباحي أو يضم مواد غير مقبولة، ومعظم مرسلي السبام لا يهتمون بأن هذه المواد قد تصل إلى يد الأطفال. يمكن أن يساعد ترشيح السبام بإبعاد البريد التافه الذي يتضمن المواد الإباحية والجنسية الفاضحة عن صندوق بريد أطفالك. انظر إلى الفصل السادس. "فقط قل لا للسبام". لمزيد من المعلومات حول التعامل مع السبام.

بالإضافة إلى ذلك يمكنك أن ترسل تقارير عن مرسلي السبام الذين يرسلون البريد الإلكتروني التافه الإباحي إلى أطفالك. لكي ترسل تقريراً، اذهب إلى موقع الوب للمركز الوطني للأطفال المفقودين والمستغلين (www.missingkids.com). انقر الارتباط CyberTipline على الجانب الأيسر من الصفحة، مرر إلى الأسفل إلى الترويسة Unsolicited Obscene Material sent to a Child، ثم انقر الزر Report. قد لا يؤدي تقريرك إلى بدء عملية تحري فورية، ولكن إذا تم تسجيل عدد كافٍ من الشكاوي، فقد تساهم في وصول مرسل السبام إلى السجن.

2-8 المستغلون الجنسيون والإنترنت

إنها حقيقة مؤسفة في الحياة الحديثة أن المستغلين الجنسيين يستخدمون الإنترنت – وخصوصاً غرف المحادثة على الوب – للبحث عن ضحاياهم. وفقاً لتقرير 2000 من مركز أبحاث الجرائم ضد الأطفال، يوجد واحد من خمسة مستخدمي إنترنت يافعين حصلوا على

دعوات من مواقع جنسية غير مرغوبة. و3 بالمائة من هذه النسبة أرسلوا تقـارير باسـتقبال "دعوات غير مطلوبة" من أجل الاتصال بدون الوب. وكان عمر ربع الأولاد الذين تم دعوتهم بين 10 و13 عاماً، في حين أن 77 بالمائة منهم بين 14 و17 عاماً. (انظر إلى القسم "مـوارد مساعدة" من أجل معرفة الارتباط إلى هذا التقرير).

وتتفاقم هذه المشكلة لأن الأطفال قد يكونوا أقل حذراً على الإنترنت مما هم عليـه في العالم الحقيقي، فمزودات الإنترنت تقدم إحساس خاطئ بالمجهولية والأمان. وهكـذا فقـد يجرؤون على الانخراط في محادثات وإقامة علاقات لن يقوموا بها شخصياً. بالإضافة إلى ذلك، يمكن خداع الأطفال اليافعين بسهولة أكبر والحصول على ثقتهم كأصدقاء على الوب.

ولكن قبل أن تنـزع سلك الهاتف من خلف الكمبيوتر، يمكنك أن تتخـذ خطـوات لتحمي أطفالك عندما يتواجدون على الوب. الشيء الأول والأهم أن تتحدث إليهم. استخدم لغة مناسبة لعمرهم لتناقش المشكلة، وتشجعهم على اللجوء إليك إذا واجهوا أي مشكلة على الإنترنت تجعلهم غير مطمئنين. وراقب ما يفعله أولادك على الوب. كما ذكرنا سابقاً، يمكنك أن تنفذ ذلك بالمراقبة الفيزيائية وباستخدام برمجيات مخصصة. سوف ندخل في تفاصيل مشكلة الاتصالات غير المناسبة والحلول المقترحة في بقية هذا القسم.

منع الاتصالات غير المطلوبة

بمعرفة طريقة عمل المستغلين الجنسيين، يمكنك أن تعرّف أولادك بسهولة أكـبر علـى علامات الخطر. وإذا كنت تراقب نشاطات أطفالك على الـوب، سـوف تتعـرف علـى الاتصالات المشبوهة حالاً.

وفقاً لتقارير FBI، يتحول المستغلون الجنسيون غالباً في غرف المحادثة لإقامة الوصلات مع الأطفال. إن الطبيعة المفتوحة لغرف المحادثة تجعل من السهل إقامة المحادثات على الـوب، والتي تبدأ بنقاش جدي حول الثقافة، الموسيقا والمواضيع الأخرى التي تهم الأطفال. ومع الزمن، قد يقيم المستغل علاقة ودودة بالرعاية والتأثير العاطفي وحتى بتقديم الهدايا. وبعد أن يحصـل المستغل على ثقة الطفل، ينتقل إلى محادثات إضافية على وسائط أكثر خصوصية، مثل البريـد الإلكتروني، الرسائل الفورية وحتى الاتصالات الهاتفية. عند هذه المرحلة يبدأ بتقديم المواضـيع الجنسية أو مشاركة المواد الفاضحة، بما في ذلك المواد الإباحية للأطفال. قد يحاول المستغل في النهاية أن يعقد لقاءات مع الضحايا؛ فقد ورد في تقارير FBI أن أحد المجرمين بعث بتـذاكر الطائرة ليشجع الضحية على عقد اللقاء.

قد يخطر ببالك أن تمنع الوصول إلى غرف المحادثة نهائياً، لكن هذا الحل غـير واقعـي بوجود الوصول الهائل إلى الإنترنت. فيمكن للأطفال ممارسة نشاطهم على الوب في المدرسة، في المكتبة، في بيت صديق لهم، في مقاهي الإنترنت وفي المنـزل عندما لا تكـون موجـوداً.

بالإضافة إلى ذلك، فالمحادثة والرسائل الفورية قد تكون طريقة مفيدة لتطوير المهارات الاجتماعية. لذلك بدلاً من نزع مأخذ الهاتف، استفد من التوصيات التالية لمساعدتك على جعل الكمبيوترات المنزلية آمنة وتعليم أطفالك الطريق الأفضل لكي يكونوا مستخدمي إنترنت أذكياء.

- تحدث مع أطفالك عن الأخطار المحدقة بالإنترنت، اطلب منهم أن يخبروك إذا كان لديهم أي اتصالات غير مطمئنين من أجلها. وإذا كنت محتاراً بطريقة بدء النقاش، انظر إلى NetSmartz.org، الذي يموله مركز الأطفال المفقودين والمستغلين. يقدم NetSmartz.org معلومات حول أمن الوب للأطفال واليافعين، وهو مورد مهم للآباء.
- أرشد أولادك بأن لا يصرحوا عن أسمائهم، أعمارهم، عناوينهم أو أرقام هواتفهم في غرف المحادثة، البريد الإلكتروني، الرسائل الفورية وهكذا. يجب أن يحجموا أيضاً عن وضع صورهم الشخصية على الوب.
- إذا أمكن الأمر، ضع كمبيوترك في منطقة عبور في المنزل، مثل غرفة المعيشة. راقب نشاط أطفالك على الوب، بما في ذلك البريد الإلكتروني ومواقع الوب التي زاروها.
- راقب علامات الخطر، كما هو مبين في الشريط الجانبي "علامات تدل على احتمال تعرض أطفالك إلى خطر على الوب" في نهاية هذا الفصل.
- استفد من مزايا التحكم الأبوي المتوفرة من مزود الخدمة، في برامج الاستعراض ومحركات البحث، وفي البرمجيات الأخرى.

إرسال تقرير عن الدعوات الجنسية

توصي FBI بإرسال تقرير إذا استقبل طفلك أو أي شخص آخر في المنزل مواد إباحية للأطفال، إذا كان عمر طفلك أقل من 18 عام وتلقى دعوة جنسية من شخص يعرف بأن عمره أقل من 18 أو إذا استقبل مواد فاضحة من شخص يعرف بأن عمره أقل من 18.

يمكنك أن ترسل تقارير عن هذه الجرائم إلى قسم الشرطة المحلية وFBI. (يمكنك الاتصال بالرقم 202-324-3000. لتعرف المكتب الأقرب إليك اذهب إلى www.fbi.gov/contaet/fo/fo.html). يمكنك أن تستخدم أيضاً CyberTipline الموجود على الجانب الأيسر من صفحة البدء للمركز الوطني للأطفال المفقودين والمستغلين في الموقع www.miss.ingkids.com لكي ترسل تقريراً بالحادثة.

تلحظ FBI أيضاً أنه في حال حدوث أي من هذه السيناريوهات وأرسلت تقريراً بها، يجب أن تغلق كمبيوترك وتتركه على حاله. لا تحذف أو تنسخ أي ملف أو صورة. فسوف يأتي وكيل تحري ويأخذ الكمبيوتر من أجل الفحص الشرعي وهي عملية قد تستغرق أيام أو أسابيع.

برمجيات مراقبة الإنترنت

بالإضافة إلى التحدث مع أطفالك حول الأخطار الكامنة، فإن برمجيات مراقبة الإنترنت يمكن أن تساعد على تطبيق القيود ومراقبة نشاطات أطفالك على الوب. قد يتحفظ بعض الناس على التجسس على نشاطات أطفالهم على الإنترنت كنوع من التدخل الأبوي السافر. بينما يرى فيها الآخرون تحذيراً مسبقاً، مثل خوذة الدراجة الهوائية وحزام السيارة. وتتعلق الدرجة التي تحدد بها وتراقب نشاطات أطفالك بعوامل مختلفة، بما في ذلك عمر طفلك (الأولاد الأكبر هم أذكى على الأغلب ويمكنهم الالتفاف على مرشحات محركات البحث وبرامج الاستعراض البسيطة)؛ تقييمك للمخاطر التي يواجهونها؛ والوقت، الجهد والنقود التي ترغب بالاستثمار بها في هذه القضية.

بحث القسم "ترشيح المواد غير المرغوبة" في المرشحات المجانية والسهلة. ويبحث هذا القسم في البرمجيات التي تم تصميمها لتطبيق التحكم الأبوي وتقديم إطار لكي يستعرض الأطفال الوب. تقدم هذه الفئة من البرمجيات وسائل تحكم شاملة ومجموعة كبيرة من المزايا بالمقارنة مع الخيارات التي تم نقاشها سابقاً، لكن يجب أن تدفع لقاء هذه الإمكانيات الإضافية.

كيف يجب أن أختار؟

توجد عدة معايير لاختيار برمجيات مراقبة الإنترنت. المعيار الأول هو شمولية وسائل التحكم. تشمل المناطق التي تحتاج إلى تحكم بها استعراض الوب والمحادثة على الوب والرسائل الفورية. يجب أن يكون المنتج الشامل قادراً على ترشيح برامج استعراض الوب الرئيسية وبرامج الرسائل الفورية. ويجب أن يهتم المنتج الجيد بالبحث عن الصور في محركات البحث إما بترشيح نتائج البحث غير المقبولة أو بتحديد المستخدم بمحرك بحث مختبر لا يعرض النتائج غير المقبولة. وقد تكون مهتماً أيضاً بترشيح ومراقبة البريد الإلكتروني.

عند تقييم برنامج، تذكر الفروق بين الترشيح والمراقبة. فالترشيح يحجز المواد غير المقبولة أو يستبدلها بالحروف X أو بنقاط. أما المراقبة فتدعك تنظر إلى ما يفعله أولادك على الوب (على سبيل المثال، مشاهدة مواقع الوب التي زاروها أو تسجيل الرسائل الفورية كاملةً).

إلى جانب وسائل التحكم المحددة، يجب أن تطلع أيضاً على طرق المرشحات المختلفة، وخصوصاً مع مواد الوب. النظام الأبسط هو لائحة سوداء بالمحددات URL لمواقع الوب التي تحتوي على مواد غير مقبولة أو بالكلمات الأساسية التي تشير إلى مواد غير مقبولة. تنشئ هذه اللوائح السوداء عادةً الشركة التي تصنع برمجيات التحكم الأبوي. وهي تغطي نطاق من الفئات، بما في ذلك المواد الإباحية، العنف، الكحول والمخدرات وهكذا. وتظل اللوائح فعالة طالما بقيت اللائحة شاملة. على كل حال، نظراً لحجم وقدرة الإنترنت على التحول، تظهر مواقع جديدة باستمرار وتتلاشى المواقع القديمة. وهكذا، عند مقارنة المنتجات، يجب أن تبحث

عن الأنظمة التي تحدّث لوائحها بشكل دوري. تسمح معظم الأنظمة بإضافة مجموعاتك الخاصة من المواقع المحظورة والمسموحة.

يوجد خيار آخر بمسح مواقع الوب قبل عرضها في برنامج الاستعراض. قد يبحث هذا المسح عن اللغة غير المقبولة أو إذا كانت الصور موجودة، يحاول أن يقيّم نوعية الصورة (على سبيل المثال، بفحص الوجوه، الأشكال والجلد في الصور). ومن المنتجات المذكورة في الجدول 8-1، يستخدم EnoLogic NetFilter Home تحليل الصور لكي يحجز الصور الإباحية في الوقت الحقيقي. إن تحليل الصور مفيد لكشف المواد غير المقبولة بدون استعادة لائحة سوداء، لكنه يحجز المواقع غير المؤذية أيضاً. قد تريد أن تبحث عن حل يسمح للآباء بتغييره للسماح ببعض المواقع التي تريد حجزها عن طريق الخطأ.

تسمح معظم برمجيات التحكم الأبوي أيضاً بتحديد الوقت الذي يقضيه أطفالك على الوب، مرشحات الحجز أو الرسائل الفورية والمحادثة تمنع البرامج من تحميل الملفات، وتمنع الأطفال من إدخال المعلومات الشخصية مثل أرقام الهواتف.

تأتي بعض البرامج الأمنية مع تحكم أبوي محدود ومبيت، فالحزمة Norton Internet Security التي تضم أيضاً جدار نار، برمجيات مضادة للفيروسات، برمجيات مضادة للسبايوير ومزايا أمنية مهمة أخرى، تضم أيضاً بعض إعدادات التحكم الأبوي لكي تحجز الوصول إلى الموارد غير المرغوبة. وعند تأهيلها يحجز مواقع الوب بالاعتماد على لائحة الفئات التي تعدها Symantec، وتضم الجنس، التعري، المخدرات والعنف. وبالعكس، يمكنك أن تحجز المستخدمين بلائحة من مواقع الوب المسموحة وتحجز كل المواقع الأخرى. (قد يكون هذا الإعداد متطرفاً، على الأقل من أجل الأطفال الأكبر سناً، الذين يستحيل أن يتوقع المرء معرفة كل موقع يريدون الوصول إليه). يمكنك أن تحجز أيضاً برامج محددة من الوصول إلى الإنترنت وتقيد مجموعات العمل.

لاحظ أن جميع برمجيات التحكم الأبوي تعتمد على حسابات المستخدمين التي يتم إسنادها إلى كل شخص يستخدم الكمبيوتر. وإذا عرف أطفالك باسم حساب وكلمة مرور شخص بالغ، يمكنهم اجتياز إجراءات التحكم الأبوي (بافتراض أنك منحت الأشخاص البالغين إمكانية الوصول بدون ترشيح). تقدم بعض المنتجات آلية صامتة بحيث لا يرى أطفالك رمز المنتج في شريط النظام. قد يكون الإعداد الصامت مفيداً، إذا كان لديك أطفال أكبر سناً وأكثر خبرة بالكمبيوتر وقد يحاولون الالتفاف على القيود التي تضعها.

تمثل المنتجات المذكورة في الجدول 8-1 عدد قليل من الحلول للتحكم الأبوي. يمكنك أن تجد مقالات جيدة عن برمجيات الأبوي في PC Magazin (www.pcmagazine.com) وفي /http://internet-filter-review.toptenreviews.com. في منتصف العام 2005 كانت أسعار برمجيات التحكم الأبوي المستقلة تتراوح بين 29.95$ و55$، ولكن العروض الخاصة والمساومات تؤثر على السعر النهائي.

الجدول (8-1):

برمجيات تحكم أبوي مختارة			
المنتج	البائع	موقع الوب	المزايا
ContentProtect	ContentWatch	www.contentwatch.com	تحليل موقع الوب بالزمن الحقيقي، يحجز الوصول إلى المحادثة، يحدد الزمن، يسجل النشاطات، يغطي كلمات المرور وأكثر من ذلك.
CyberPatrol	SurfControl	www.cyberpatrol.com	لوائح سوداء ولوائح بيضاء بمواقع الوب، تحليل نص موقع الوب بالزمن الحقيقي، ترشيح نتائج محرك البحث من الصور، حجز المحادثة والرسائل الفورية، تحديد الزمن، حجز مواقع السبايوير وأكثر من ذلك.
CYBERSitter	Solid Oak Software	www.cybersitter.com	لوائح سوداء ولوائح بيضاء بمواقع الوب، حجز الصور من محرك البحث، تحديد الزمن تسجيل محادثات الرسائل الفورية على AOL وYahoo!Messenger، النمط الصامت، وأكثر من ذلك.
EnoLogic NetFilter Home	EnoLogic	www.enologic.com	تحليل الصور والنصوص في مواقع الوب، لوائح سوداء بالمستخدمين، يحجز المحادثة، يحجز المعلومات الخاصة، يمنع نقل الملفات الكبيرة، يكشف الملفات MP3، وأكثر من ذلك.

برمجيات تحكم أبوي مختارة			
المنتج	البائع	موقع الوب	المزايا
NetNanny	LookSmart	www.netnanny.com	لوائح سوداء ولوائح بيضاء بمواقع الوب، سجل بالنشاطات، ترشيح النصوص في برامج الاستعراض. المحادثة، البريد الإلكتروني، ومجموعات العمل، تحديد الزمن، يحجز الوصول إلى المحادثة والرسائل الفورية وأكثر من ذلك.

3-8 الأغنية 3000$ ومشاكل مشاركة الملفات الأخرى

تسبب النقود معظم المشاكل الأمنية التي نواجهها عند استخدام الإنترنت. وهذه هي الحال أيضاً في هذا القسم، ولكن بشكل آخر: بدلاً من الوقوع ضحية لجرائم مجرمي الإنترنت الأذكياء، فإن المؤسسات العملاقة تشعر بأنها الضحية وأن المجرم هو أنت. حسناً، قد لا تكون أنت شخصياً ولكن أي شخص يستخدم الإنترنت للبحث، تحميل ومشاركة الموسيقا والأفلام التي تملك حقوق نسخ وبدون أن يدفع فلس واحد للتصريح عن استخدامه. فهذه المؤسسات، هيئة صناعة التسجيلات في أمريكا (RIAA) وهيئة الصور المتحركة في أميركا (MPAA)، تدعي أنها فقدت ملايين الدولارات في مبيعات التسجيلات والأفلام بسبب تقنية تدعى مشاركة الملفات.

تنفذ تقنية مشاركة الملفات ما يدل عليه اسمها: تسمح للمستخدمين بمشاركة الملفات. ومعظم هذه الملفات هي ملفات موسيقا في التنسيق MP3 عادةً، وهو تنسيق ترميز وضغط الإشارات الصوتية. وتشمل التنسيقات الرقمية الشائعة الأخرى Windows Media Audio (AAC) الذي تستخدمه حافظات iTunes ومشغلات iPod أبل. تسمح برامج مشاركة الملفات أيضاً بمشاركة أي نوع آخر من الملفات الرقمية، بما في ذلك الأفلام، المستندات، الصور والبرمجيات.

يتم تطبيق مشاركة الملفات على شبكات ند إلى ند (P2P). تتألف هذه الشبكات من عقد منفردة، مثل الكمبيوترات، موصولة عبر شبكة. تقابل الشبكات P2P الشبكات مستضاف/ملقم. في النوع الأخير من الشبكات ترسل وتستقبل مجموعة من المستضافات البيانات إلى ومن ملقم مركزي. يمكن إعداد هذا الملقم لكي يسمح للمستضافات بمشاركة

الملفات أو الموارد نفسها، لكن المستضافات لا تتصل مع بعضها بشكل منفرد؛ الملقـم هـو المستودع الرئيسي للمعلومات. وعلى الأغلب فإن الشبكة المستخدمة في مكتبـك تسـتخدم النموذج مستضاف/ملقم.

وبالمقابل، فإن الشبكات ند إلى ند لا تحتوي على ملقم رئيسي؛ ويمكن أن تحمّل كـل عقدة أو ند الملفات من أنداد أخرى وتخدم الملفات إلى كمبيوترات أخرى. ويمكنها أن ترتب الكمبيوترات وفقاً لسعة الشبكة.

لقد كانت Napster الشبكة P2P الأولى التي تحظى بانتباه العموم. وكانـت إحـدى الشبكات P2P الرئيسية الأولى التي تعرضت للهجوم من صناعة التسجيلات. فقـد قاضـت Napster لتحميلها ومشاركة الأغاني بدون الدفع من أجلها. تم إغلاق Napster في النهاية، لكنها عادت للظهور كمخزن موسيقي على الوب يدفع الرسوم المناسبة لصناعة التسجيلات.

على كل حال، بالنسبة إلى مشاركة الملفات والشبكات P2P، فقد خرجـت القطـة الرقمية من الكيس. فالشبكات P2P مثـل Kazaa، Grokster، Gnutella، Morpheus ومئات غيرها تسمح للمستخدمين بمشاركة والبحث عن الموسيقا، الأفلام، والمـواد الرقميـة الأخرى مجاناً.

بالطبع، لا يوقف ذلك RIAA من محاولة إعادة القطة إلى الكيس. في هذه المرحلـة، لم تملك RIAA التقنية اللازمة؛ فقد فشلت العديد من المحاولات لتشفير وحمايـة التسـجيلات الصوتية الرقمية بطرق أخرى من النسخ والتوزيع. لكن القانون كان بجانب RIAA: إن تحميل أو جعل المواد ذات حقوق النسخ متاحة للتحميل بدون إذن صاحب حقوق النسخ هو عمل غير قانوني. لكن الشبكات P2P نظامية، ومن هنا يبدأ تعقيد المشكلة.

تتابع RIAA وMPAA معركتهم القانونية على جبهتين. على الجبهة الأولى يلاحقـون بائعي البرمجيات P2P التي تسمح بالتعدي على حقوق النسخ. وعلى الجبهة الثانية، يلاحقون المؤسسات (على الأخص، الجامعات) والأفراد الذين يشاركون بشكل غير قانوني المواد ذات حقوق النسخ.

أعلنت RIAA في نيسان 2005 عن جولة أخرى من الدعاوى ضد الأفـراد المتـهمين بمشاركة الملفات غير النظامية. يقول أحد الصحفيين أن العدد الكلي للأشـخاص الـذين تم اسـتدعائهم للمحاكمـة في هـذه الجولـة بلـغ أكثـر مـن 10000 (انظـر إلى http://sharenomore.bloyspot.com/). في عام 2003، RIAA قاضت مئات الأشخاص على مشاركة الملفات الموسيقية بشكل غير نظامي. وقد بلغت الغرامة بشكل تقريبي 3000$.

تتابع MPAA أيضاً مقايضة الملفات. فقد بدأت جولة أولى من الـدعاوى في تشـرين الثاني 2004، وتبعتها جولة ثانية في كانون الثاني 2005.

وقّع الرئيس جورج بوش في نيسان 2005 على مرسوم ترفيه العائلة وحقوق النسخ. كعقوبة لقراصنة المواد الرقمية، ينص القانون على أن شخص يتم توقيفه لوجود فيلم أو أغنية أو برنامج غير مرخص على كمبيوتره قد يواجه ثلاث سنوات في السجن أو غرامة تصل حتى 250000$.

أخيراً، بدأت المحكمة العليا بالاستماع إلى المرافعات في قضية Inc.U.Grokster LTD، MGM Studios في بداية ربيع 2005. وجوهر المشكلة هو أن MGM، ستوديو أفلام، يدّعي أن Grokster، برنامج مشاركة ملفات P2P، صالح لجميع عمليات التعدي على حقوق النسخ ويؤهل المستخدمين بآلية لمشاركة المواد محفوظة حقوق النسخ. القضية معقدة وسوف تتضمن كثيراً من المداولات قبل أن تصدر المحكمة حكمها. يذكر العديد من المراقبين السابقة التي قاضت فيها الشركة Universal الشركة Sony من أجل التعدي على حقوق النسخ، مدعيةً أن تقنية Betamax من Sony قد سمحت للمستخدمين بتسجيل برامج التلفزيون بشكل غير شرعي. وقد أدانت المحكمة العليا الشركة Universal بأن الشركة Sony لم تكن مسؤولة عما فعله المستخدمين بتقنيتها. وقد أشارت المحكمة أيضاً إلى أن عمليات المستخدمين (تسجيل برامج التلفزيون لمشاهدتها لاحقاً) هي استخدام مشروع للمواد محفوظة حقوق النسخ.

على كل حال، قد تصعب مناقشة أن مشاركة الأغاني محفوظة حقوق النسخ مع ملايين المستمعين يعتبر استخداماً مشروعاً، مع الأخذ بعين الاعتبار الخسارة الكبيرة التي يتحملها مالكو حقوق النسخ. عند كتابة هذا الفصل، لم تكن المحكمة العليا قد توصلت إلى قرارها بعد. انظر إلى القسم "Helpful Resources" من أجل ارتباط يعطي مقدمة عامة عن القضية والتداعيات الكبيرة لقرارات المحكمة المحتملة.

كيف يمكنهم العثور عليّ؟

تقدم الإنترنت إحساس خاطئ بمجهولية مستخدمي البرمجيات P2P. وكما يبين عدد الدعاوى المقامة من RIAA وMPAA، فإنهم يمكن العثور على المستخدمين المستقلين. لا يتعلق السؤال فيما إذا كان بإمكانهم العثور عليك، ولكن فيما إذا كان سيتم توقيفك في عملية تعدي على حقوق النسخ. تلاحق هذه المؤسسات حالياً المستخدمين الأكثر فظاعة. لذلك فإن فرص استهدافك من هذه المؤسسات منخفضة (بافتراض أنك لم تعد ملقم وب لتبادل الملفات الصوتية الرقمية).

ولكن كيف يمكنهم العثور على المتعدين على حقوق النسخ؟ حسناً، الطريقة الأبسط هي أن توقّع على مختلف الشبكات P2P وتجد عقدة تقوم بمشاركة المواد محفوظة حقوق النسخ. تملك RIAA وMPAA معاييرها الخاصة لاتخاذ القرار حول العقد التي ستتابعها، لكن بعد أن تقرر أي من هذه العقد سوف تتابعها، تتحقق أن العقدة تقدم المواد محفوظة النسخ بشكل غير نظامي. بعدئذٍ يمكنها العثور على العنوان IP للعقدة باستخدام مختلف أدوات البحث. وبعد أن تجد العنوان IP،

يمكنها أن تحد مزود الخدمة لهذه العقدة. ثم تقيم الدعوى "Johne Doe" ببساطة. وفقاً لمعلومـــات على موقع الوب RIAA، يمكن أن يرفع المدعون الدعاوى "Jone Doe" عندما لا يعرفون اســـم الشخص الذي يقاضونه. بعد إقامة الدعوى، يمكن أن يستدعي المدعي مزود الخدمة ISP للمثـــول أمام المحكمة والإدلاء باسم الشخص الذي يستخدم العنوان IP المحدد. لمزيد من المعلومات، انظر إلى .www.riaa.com/news/newsletter/012104_faq.asp

حاولت RIAA في دعاويها السابقة أن تنفذ هذه العملية بطريقة مختلفة. أي أنها حاولت أن تحمل مزودات الخدمة ISP على الإدلاء بأسماء مخالفي حقوق النسخ ومعلوماقم الشخصية. ولكن الشركة Verizon Online تحدت طلب RIAA، فقاضت الأخيرة Verzion ووصلت القضية إلى المحكمة العليا، والتي كانت قد أصدرت حكماً سابقاً بأنه من حق مزودات الخدمة أن تمتنع عن إفشاء هوية زبائنها. ولكن الدعوى Jone Doe هي قانونية بالكامل، ويعني ذلك أنه إذا استلم مزود خدمة طلباً في نطاق دعوى Jone Doe، فيجب أن يفصـــح عـــن اســـم المشترك ومعلوماته الشخصية.

أمور أمن P2P

بالإضافة إلى المشاكل القانونية التي تأتي من عدم الدفع لقاء استخدام الموسيقى والأفلام، يمكن أن تعرّضك البرامج P2P إلى أخطار أمنية. عندما تحمّل وتستخدم البرمجيات P2P، قد لا تلاحـــظ أنك تعرض كمبيوترك إلى الكمبيوترات الأخرى الموجودة على الإنترنت. فالمجلد الذي يحتوي على ملفات رقمية يتم مشاركتها قد يكون مفتوحاً على الإنترنت. وإذا تم إعداده بشكل غير مناســـب، يمكنك أن تفتح محرك القرص الصلب بأكمله وجميع محتوياته إلى الإنترنت. إذا كنت تستخدم جدار نار (يجب على الأغلب أن تكون قد استخدمت جدار نار) يجب أن تفتح المنافذ لتتمكن البرمجيات P2P من العمل. على كل حال، عند فتح هذه المنافذ تعرض كمبيوترك للمتدخلين السيئين.

بالإضافة إلى ذلك، كما تم نقاشه في الفصل السادس، فإن معظم التطبيقات P2P تحتوي على الأدوير الذي يتعقب سلوكك على الوب، يولد الإعلانات المنبثقة المزعجة، ويقلل من أداء كمبيوترك. وأخيراً، شرع المهاجمون والمجرمون بزرع أحصنة طروادة وبرامج المالوير الأخـــرى ضمن الملفات P2P وأطلقوا عليها أسماء طريفة أو جذابة. فتظن أنك تحصل على نسخة مـــن U2 B أو الفيلم Hitchhiker's Guide to the Calaxy، ولكن بدلاً من ذلك تثبت مسجل ضربات مفاتيح على كمبيوترك.

إذا كنت ما تزال تريد استخدام البرمجيات P2P، تأكد من أنك تســـتخدم برمجيـــات مضادة للفيروسات وبرمجيات مضادة للسبايوير لتمسح جميع الملفات الـــتي تحملـــها، وتقـــرأ تعليمات الإعداد بعناية لتتأكد من أنك تعرض على الإنترنت الملفات التي تريـــد مشـــاركتها فقط. وكما ذكرنا، فإن معظم البرامج P2P تعد بمجلد محدد على كمبيوترك لهذا الغرض.

نظامي أم غير نظامي؟

هل احترت من هذا الجدل القانوني حول مشاركة الملفات؟ يقدم الجدول 8-2 مرجعاً سريعاً لمساعدتك على فرز ما هو صحيح وما قد يعرضك للمقاضاة والتوقيف.

الجدول (8-2):

مشاركة الملفات النظامية في مقابل غير النظامية	
النظامية	**غير النظامية**
باستخدام البرمجيات P2P.	باستخدام البرمجيات P2P لتحميل ومشاركة المواد محفوظة حقوق النسخ بدون إذن.
شراء الموسيقا على الوب.	شراء الموسيقا على الوب ثم مشاركتها باستخدام البرمجيات P2P.
نسخ الملفات الصوتية الرقمية أو الأفلام التي دفعت ثمنها لتشغيلها على قرص مضغوط أو في مشغل محمول.	نسخ الملفات الصوتية والأفلام لإعادة بيعها أو مشاركتها بالشبكات P2P.

8-4 لائحة التدقيق

استخدم هذه اللائحة كدليل مرجعي للمواد المغطاة في هذا الفصل.

ما يجب أن تفعله

- الاستفادة من خيارات الترشيح لإبعاد مواد الإنترنت غير المقبولة.
- محاولة تحديد استخدام الأطفال للإنترنت على كمبيوتر موجود في منطقة عبور من المنزل كغرفة المعيشة أو المطبخ.
- الحديث مع أطفالك عن أخطار الإنترنت.
- تشجيع أطفالك على عدم وضع أسمائهم، أرقام هواتفهم، عنوان منزلهم، عناوين بريدهم الإلكتروني، وصورهم على الوب.
- مراقبة العلامات التي تدل على تعرض طفلك إلى سيطرة مستغل جنسي على الوب.

الحديث مع أطفالك عن الأمور القانونية والأمنية المقترنة مع مشاركة الملفات ند إلى ند.

ما يجب أن لا تفعله

- أن تدع أطفالك يستخدمون الإنترنت بدون إشراف.

- التصديق أن أنظمة الترشيح فعالة 100 بالمائة.
- التصديق أنه لا يمكن الالتفاف على نظام الترشيح المستخدم.

5-8 موارد مساعدة

يقدم هذا القسم موارد إضافية لمساعدتك على تعلم المزيد.

المركز الوطني للأطفال المفقودين والمستغلين هو مؤسسة غير ربحية تقدم خـــدمات إلى العائلات التي لديها أطفال مفقودين أو تعرضوا إلى إساءة أو استغلال جنسي. موقع الـــوب للمركز، www.missingkids.com، ويقدم الكثير من المعلومات عن حماية الأطفال علـــى الوب. وإذا احتجت أيضاً لإرسال تقارير على الوب عن الـــدعوات الجنســـية أو المواضـــيع الأخرى، فإن موقع الوب CyberTipline هو مكان ممتاز لتبدأ منـــه. تجـــد الارتبـــاط إلى CyberTipline على الجانب الأيسر من صفحة البدء.

لكي تقرأ التقرير "ضحايا الوب: تقرير عن شبيبة الأمة" من مركز أبحاث الجرائم ضـــد الأطفال، اذهب إلى www.missingkids.com/en_US/publications/NC62.pdf.

لمزيد من المعلومات عن طريقة الحديث عن الأمن على الوب مع أولادك أو مع المراهقين، اذهب إلى www.netsmartz.org. ويمكن أن يستعرض الأطفـــال الأكثـــر عمـــراً الموقـــع www.metsmartzkids.org من أجل دورة تعليمية على الوب عن أمان الإنترنت. يشارك في دعم NetSmartz المركز الوطني للأولاد المستغلين والمفقودين ونوادي الصـــبية والصـــبايا في أميركا.

تنشر FBI "دليل الأب إلى أمان الإنترنت"، ويقدم توصيات مساعدة للمحافظة علـــى أمان أطفالك على الوب. كما يفصل أيضاً الخطوات الضرورية إذا اشتبهت بأن طفلك يتصل مع مستغل جنسي. اذهب إلى www.fbi.gov/publications/pguide/pguidee.htm لتقرأ الدليل.

لكي تقرأ المزيد عن قرصنة الموسيقا من منظور هيئة صناعة التســـجيلات في أميركـــا (RIAA)، اذهب إلى www.riaa.com/issues/privacy/default.asp. وقد تريد الإطلاع على الارتباط Penalties "الجزاء" في الزاوية العليا اليمنى.

كتبت جولي هيلدن مقدمة عامة ممتازة عن القضية MGM v. Grokster المعروضة حالياً علـــى المحكمـــة العليـــا. يمكنـــك أن تقرأهـــا في /www.cnn.com/2005/LAW/02/16 hilden.fileswap/.

علامات تدل على أن طفلك قد يكون في خطر على الوب

على الرغم من حذرك، فقد يتعرض أطفالك إلى استغلال جنسي أو إلى إزعاجات المواد الجنسية على الوب، لقد شرحت FBI سبع علامات يمكن أن تشير إلى أن طفلك في خطر على الوب. وتم صياغة هذه العلامات السبعة من "دليل الأب إلى أمان الإنترنت" من FBI. يمكنك أن تجد ارتباطاً إلى الدليل الكامل في القسم "موارد مساعدة". مع أن هذه العلامات مساعدة لكن يجب أن يتذكر الآباء أن علامتين منها (قضاء أوقات طويلة على الإنترنت والانعزال عن العائلة) يمكن أن تعبران عن سلوك طبيعي تماماً، وخصوصاً للمراهقين ومن هم على وشك الدخول في سن المراهقة. وإذا اشتبهت بوجود مشكلة، تحدث مع طفلك قبل أن تقفز إلى الاستنتاجات.

- يقضي طفلك أوقات طويلة باستخدام الإنترنت. ويختلف معنى التعبير "أوقات طويلة" من عائلة إلى عائلة، لذلك يجب أن تستخدم حكماً منطقياً. على كل حال، تصرح FBI أن نشاط مستغلي الأطفال يزداد في الأمسيات والعطل الأسبوعية.
- تجد مواد إباحية على كمبيوتر طفلك. فقد يستخدم المستغلون الجنسيون المواد الإباحية، بما في ذلك المواد الإباحية للأطفال، لكي يبدؤوا نقاشات جنسية مع الأطفال أو لإغراء الضحايا المحتملين. إذا اكتشفت أن أحداً قد أرسل مادة إباحية (خصوصاً مادة إباحية للأطفال) إلى طفلك، يجب أن تتصل بقسم الشرطة وFBI (اتصل بالرقم 202-324-3000 أو اذهب إلى www.fbi.gov/contact/fo/fo.htm لتجد المكتب الأقرب إليك). ويمكنك أن تستخدم CyberTipline الموجود على الجانب الأيسر من صفحة البدء في www.missingkids.com لكي ترسل تقرير عن الحادثة. إذا كنت ترسل تقريراً عن المواد الإباحية إلى قسم الشرطة، ينصح FBI بأن تغلق كمبيوترك وتتركه على حاله. ويجب أن تعلم أن ضابط الشرطة قد يأخذ كمبيوترك لإجراء فحص شرعي.
- يتلقى طفلك مكالمات هاتفية من الغرباء أو يجري اتصالات هاتفية مع أرقام غير معروفة. يحاول المستغلون الجنسيون غالباً أن ينقلوا الاتصال من غرف المحادثة إلى وسط أكثر خصوصية. ويحاول بعضهم أن يورطوا الأطفال في اتصالات هاتفية جنسية أو يستخدموا الهاتف لترتيب لقاء شخصي.
- يرسل غريب إلى طفلك رسائل، هدايا أو طرود. فقد يتابع المستغل الجنسي عملية الاتصال ويستخدم الهدايا لمساعدته في بناء علاقة.
- يغلق طفلك الكمبيوتر أو يغير الشاشة المعروضة بسرعة عندما تدخل إلى الغرفة. هذه علامة بأن طفلك يشاهد شيئاً لا يريدك أن تراه.

- انسحاب طفلك من العائلة. قد يحاول المستغل الجنسي أن يعزل طفلك عن بقية العائلة لكي يسهّل بناء علاقته مع الطفل. وفي السيناريو الأسوأ، قد يكون ذلك علامة بـــأن طفلك قد وقع ضحية.
- يستخدم طفلك حسابات بديلة على الوب. فقد يمكنك الوصول إلى حساب طفلـــك الرئيسي على الوب، لكنه من السهل جداً على طفلك إقامة حسابات بريد إلكتروني ورسائل فورية قد لا تعرف عنها شيئاً. وقد يتم استخدام هذه الحســـابات المنفصـــلة بشكل مهذب، ولكن يمكن استخدامها أيضاً للاتصالات الخاصة بين المستغل والضحية المحتملة.

لكي تقرأ نسخة كاملة عن دليل FBI للتجول في الإنترنت بأمان للعائلات، والذي يشرح علامات الخطر المذكورة، انظر إلى القسم "موارد مساعدة".

الفصل التاسع

أمن الاتصالات اللاسلكية وVoIP

لقد كانت الكمبيوترات والهواتف أجهزة مستقلة. أما في هذه الأيام فيصعب وضع حدّ يفصل بينها، وخلال السنوات الخمس التالية سوف تتلاشى أي حدود فاصلة بينها غالباً. لقد أصبحت الكمبيوترات جوالة بفضل التقدم المحقق في الكمبيوترات اللاسلكية والهاتف على الإنترنت، وأصبح ممكناً إجراء اتصال هاتفي من كمبيوترك. وفي هذه الأثناء، فإن الهواتف الخليوية، المساعدات الرقمية الشخصية (PDA)، وأجهزة البريد الإلكتروني اللاسلكية تعتمد على المزايا، الوظائف، وطاقة المعالجة للكمبيوترات المكتبية.

يوجد لهذا التطور الكثير من الجوانب الجيدة. فالتقنية اللاسلكية تقدم المزيد من القدرة على التجوال والتكيف في المنزل، وتجعل الوصول إلى الإنترنت سهلاً خارج المنزل. في هذا الوقت، تقتصر الكمبيوترات اللاسلكية على بعض الأماكن المهمة العامة. ولكن في النهاية سوف نحصل على النوع نفسه من تغطية الإنترنت اللاسلكية للكمبيوترات التي تحصل عليها من مزود الخدمة الهاتفية الخليوية. تقدم تقنية الصوت عبر IP (VoIP) حالياً خدمة هاتفية رخيصة بتحويل كمبيوترك إلى هاتف وتوجيه المكالمات الهاتفية عبر الإنترنت.

بمناسبة الحديث عن الخدمة الهاتفية، فإن الإصدارات الخليوية تحقق تطوراً فريداً فيضيف البائعون المزايا والخدمات مثل الرسائل النصية (من كان يعتقد بأن استخدام الهاتف لإرسال رسائل نصية مقروءة سوف يصبح شائعاً؟)، الصور الرقمية، والوصول إلى الإنترنت. بالإضافة إلى ذلك، فإن الأجهزة مثل BlackBerry، الذي يزود خدمة البريد الإلكتروني اللاسلكي أثناء الحركة، وPalm Pilots، وهي منظمات رقمية، سوف تستخدم المزايا الهاتفية، وتنهي الحدود الفاصلة بين أجهزة الاتصالات المحمولة. وفي المستقبل (على الأقل كما يحلم بذلك بعض المعلنين)، سوف تبث الأعمال المحلية دعاياتها وعروض الأسعار إلى هاتفك الخليوي عند مرورك بجوار مخازنها.

بالطبع، كما تكون قد خمنت ذلك، يجب أن تتم الموازنة بين الجوانب المفيدة للتقنية مع المساوئ الأمنية. والمساوئ، خصوصاً في التقنية اللاسلكية، عظيمة الأهمية. تمتد المشاكل مـــن المتطفلين اللاسلكيين الذين يقبضون على وصلة الإنترنت التي تستخدمها ويبدؤون بـــالتجول على الوب إلى المجرمين الذين يسرقون المعلومات الحساسة. ومع تحول الهواتـــف الخليويـــة إلى كمبيوترات محمولة، فسوف تتعرض إلى العديد من المشاكل الـــتي تصـــيب الكمبيـــوترات الشخصية (فيروسات الهواتف الرقمية موجودة). وعندما يتحول كمبيوترك إلى هاتف يستخدم VoIP، فسوف يتحمل بعض المساوئ، وبعضها يتضمن مساوئ أمنية (الخدمة 911). يبحث هذا الفصل في الأخطار المحدقة بهذه التقنيات الجديدة.

1-9 عمل الشبكات اللاسلكية

في هذه الأيام، يوجد في كثير من المنازل أكثر من كمبيوتر واحد يحتاج إلى الوصول إلى الإنترنت في وقت ذاته. وهكذا تزدهر الشبكات المنـــزلية عبر كل البلاد. تـــربط الشـــبكة المنـــزلية بين عدة كمبيوترات فيمكنها تبادل الملفات ومشاركة الوصول إلى الإنترنت. ويمكن توصيل الشبكات المنـــزلية سلكياً أو لاسلكياً. إن الشبكات اللاسلكية شائعة لأنها لا تحتاج إلى تمديد الكابلات إلى جميع الكمبيوترات في المنـــزل، وتتشارك عائلتك بوصـــلة الإنترنـــت في الوقت ذاته وكل من غرفته، غرفة المعيشة، غرفة المكتب وحتى من خارج المنـــزل (وحســـب قوة نقطة الوصول).

تحتاج الوصلة اللاسلكية الأساسية إلى مكونين: بطاقة لاسلكية أو رقاقة في كمبيوترك، ونقطة وصول (AP)، تدعى أحياناً موجه لاسلكي. في هذه الأيام يتم إنتاج معظم الكمبيوترات المحمولـــة مع تزويدها بالقدرة اللاسلكية. إذا كان لديك كمبيوتر محمول قديم، يمكنك أن تشـــتري بطاقـــة لاسلكية فتضيف إليه إمكانية الاتصال اللاسلكي. يمكن أن تربط نقطة الوصـــول مـــع أي آليـــة تستخدمها للوصول إلى الإنترنت: جاك هاتفي، مودم DSL أو مودم كابل. يمكن وصـــل عـــدة كمبيوترات بالأمواج الهوائية إلى نقطة وصول واحدة. يشمل الباعة الرئيسيون للمنتجات الشـــبكية اللاسلكية المنـــزلية Linksys، Belkin، D-Link وNetGear.

تعتمد الشبكات اللاسلكية المنـــزلية في هذه الأيام على مجموعة من المعـــايير الـــتي تـــدعى Wi-Fi، وهي اختصار لدقة الاتصالات اللاسلكية. يتم رعاية Wi-Fi مـــن معهـــد المهندســـين الكهربائيين والإلكترونيين (IEEE)، التي تراقب المعايير التقنية لكي تضمن العمـــل المتبـــادل بـــين منتجات الشركات المختلفة. تتألف Wi-Fi من مختلف المعايير التي يتم وضعها باســـتخدام نظـــام رقمي يدعى 802.11، وهو اسم اللجنة التي تنشئ معايير الشبكات اللاسلكية. يتحدث هذا الفصل عن أربعة معايير IEEE: 802.11b، 802.11g، 802.11a و802.1x. الأحرف b، g وa تـــدل على معايير قياسية لإرسال البيانات. يشرح 802.1x إطار عمل لتبادل معلومـــات التحقـــق مـــن

الصحة بين الأجهزة في الشبكة اللاسلكية. سوف تتعلم المزيد عن 802.1x لاحقاً في هذا الفصل.

تختلف المعايير b، g وa بعدة أوجه، بما في ذلك السعة (حجم البيانات التي يمكن إرسالها وبأي سرعة)، المجال (المسافة التي يمكن للإشارة أن تجتازها)، الطيف الراديوي الذي تستخدمه، وطريقة التعامل مع مشاكل التداخل المغناطيسي. (تعاني الإشارات الراديوية من التداخل بسبب الكائنات الفيزيائية مثل الجدران، العوارض، والمظاهر الطبيعية مثل التلال، بالإضافة إلى التداخل من الأمواج الكهرمغناطيسية المولدة من الأجهزة مثل أفران المايكرويف).

لقد تم اعتماد المعيار 802.11b بشكل واسع، ويعني ذلك أن معظم الأجهزة اللاسلكية التي تشتريها تستخدم أو تدعم هذا المعيار. ويعني أيضاً أن معظم أماكن العامة مثل المقاهي، تستخدم هذا المعيار. يملك المعيار 802.11b معدل أقصى 11 ميغابت في الثانية ويمكنه أن يرسل ويستقبل البيانات حتى مسافة 150 قدم. على كل حال، تقدم المعايير الأحدث سرعة أكبر – حتى 54 ميغابت في الثانية – لكنها غير مدعومة من المنتجات بشكل واسع حتى الآن (ولكن ذلك يتغير بسرعة). أي أن المنتجات الجديدة تظهر بشكل دائم، وبعضها يدعم معايير متعددة ويمكنها التبديل بينها، حسب متطلبات الشبكة. إن اختيار معيار معين يعني قبول المقايضة المفروضة. على سبيل المثال، يقدم المعيار 802.11a نصف المجال الذي تدعمه المعايير الأخرى، لكنها تعمل في المجال الطيفي 5 GHZ، وهو مجال أقل ازدحاماً وبالتالي أقل عرضة للتداخل المغناطيسي. أما المعياران 802.11b وg فيقدمان سرعة أكبر ومتوفران في العديد من منتجات المستهلكين Wi-Fi والشبكات اللاسلكية العامة.. على كل حال، قد تعاني من تداخل من الهواتف اللاسلكية وأفران المايكرويف. يلخص الجدول 9-1 معايير Wi-Fi الثلاثة.

الجدول (9-1):

معايير الشبكات اللاسلكية				
المعيار	السرعة القصوى	المجال	دعم المنتج	التردد
802.11b	11 ميغابت في الثانية	100 إلى 150 قدم	دعم مسافات كبيرة في المنتجات اللاسلكية.	2.4 GHZ
802.11g	54 ميغابت في الثانية	100 إلى 150 قدم	دعم متزايد. متوافق مع 802.11b (ولكن بمعدل 11 ميغابت في الثانية فقط).	2.4 GHZ
802.11a	54 ميغابت في الثانية	25 إلى 75 قدم	تقنية جديدة مع الدعم الأقل المتوفر (حتى الآن). لا تعمل مع 802.11b أو g.	5 GHZ

2-9 الأمور الأمنية مع الشبكات WLAN المنـــزلية

تأتي الخدمات التي تقدمها الشبكات Wi-Fi (تدعى أيضاً الشبكات المناطقية المحلية اللاسلكية أو WLAN) لقاء سعر معين: انخفاض في مستوى الأمن والخصوصية. قـــد لا تلاحظ ذلك، لكن الرقاقة أو البطاقة اللاسلكية في الكمبيوتر ونقطة الوصول هي أجهزة راديوية، على الرغم من أنها تستخدم ترددات مختلفة عن الأجهزة AM/FM التقليديـــة. يمكن التقاط الإشارات من الأجهزة اللاسلكية التي تعمل في هذا المجال، وليس فقط نقطة الوصول المستخدمة. ويعرف المهاجمون هذه الحقيقة لذلك فإنهم يستخدمون برمجيات تدعى برمجيات التجسس. تسمح لهم بالتجسس على الوصلات اللاسلكية غير المشفرة. وتكافئ برمجيات التجسس عملية التنصت على الخطوط الهاتفية، ما عدا أنها تلتقط رسائل البريـــد الإلكتروني، الرسائل الفورية، وبالطبع أي كلمة مرور أو أرقام حسابات قد تســـتخدمها خلال جلسة الاتصال اللاسلكي. إن أدوات التجسس اللاسلكية هي إصدارات محدثة من أدوات التجسس اللاسلكية، التي تراقب عمليات الإرسال على الشبكات السلكية. على كل حال، استخدام أدوات التجسس اللاسلكية أسهل بكثير لأنك لا تحتاج إلى توصـــيل أسلاك أو استخدام حاك احتياطي في الشبكة – بل توصلها بالطاقة قرب شبكة Wi-Fi وتراقب حركة المرور.

بالإضافة إلى أدوات التجسس، يمكن أن يصل أي كمبيوتر يحتوي على بطاقة لاسلكية أو رقاقة ضمن المجال نفسه إلى نقطة الوصول. تقدم معظم التقنيات WLAN مجالاً حـــتى 150 قدماً، لذلك لن تسافر إشارتك إلى الصين ثم تعود أدراجها، لكن مجالها يكفي ليغطي الجيران أو أي شخص آخر يجلس في مقابل منـــزلك ويحاول الوصول إلى شبكتك. تـــذكر أيضـــاً أن الإرسال اللاسلكي لا يسافر ببساطة في خط مستقيم؛ بل يتم إشعاعه بمختلف الاتجاهات. وتمر الإشارات اللاسلكية أيضاً عبر الجدران، الأرضيات، الأسقف لذلك قد يتواجد جيرانك ضمن المجال نفسه.

لكن المخاطر التي تواجهها عند استخدامك للشبكات WLAN المنـــزلية ليست شديدة الخطورة. واحتمال أن يأتي مجرم قرب منـــزلك ويدخل إلى شبكتك اللاسلكية ليس كـــبيراً. (احتمال أن يحدث ذلك في الأماكن العامة أكبر، لكننا سوف نتطـــرق إلى هـــذا الموضـــوع لاحقاً). أما الاحتمال الأكبر فهو أن يتطفل شخص فضولي على شبكتك أو يستخدم وصـــلة الإنترنت مجاناً. كما قد يتجول بعض المتحمسين حول الجيران ويستخدمون برمجيات خاصـــة للبحث عن الشبكات اللاسلكية. يدعى ذلك حرب القيادة (يماثل هذا المصـــطلح "حـــرب الاتصالات" تقنية هجوم يتصل فيها كمبيوتر مؤتمت بلائحة طويلة من الأرقام الهاتفية بحثاً عن مودمات الكمبيوتر). تبحث حرب القيادة عن نقاط الوصول المجانية إلى الإنترنت لدى الجيران، لكن بعض حروب القيادة تسعى لاختراق الشبكات. على كل حال، تستهدف على الأغلب

الشبكات WLAN في الشركات التي لا تستخدم إجرائيات أمنية أو تستخدم إجرائيات ضعيفة.

يترك بعض الناس نقاط الوصول مفتوحة من أجل تأمين الوصول من منطقة واسعة. إذا كنت تفضل المحافظة على الخصوصية يمكنك إقفال الشبكة WLAN. ولكن في البداية، استفد من آليات التشفير المتوفرة مع نقاط الوصول. تأخذ عملية التشفير البيانات التي ترسلها من كمبيوترك إلى AP (والعكس بالعكس) وتبعثر النص فتجعله غير مقروءاً، ويمنع ذلك المستخدمين الآخرين من رؤية كل ما ترسله وتستقبله على وصلتك اللاسلكية.

توجد ثلاثة آليات عامة لتشفير بيانات WLAN: WEP (الخصوصية المكافئة السلكية)، WPA (الوصول المحمي Wi-Fi) وWPA2 (إصدار محدث من WPA يستخدم خوارزمية تشفير قوية). WPA2 هو المواصفة القابلة للتشغيل مع 802.11i، معيار لاسلكي آخر يطمح لتعزيز أمن الشبكات اللاسلكية.

ظهرت WEP مع الإصدارات المبكرة للشبكات اللاسلكية وأثبتت أنها عديمة الفائدة عالمياً، وخصوصاً لتأمين الأعمال على الشبكات WLAN.

المشكلة الكبرى مع WEP هي استخدامها السيئ لتقنية التشفير، أي أنها تستخدم مفاتيح تشفير عبر فترة طويلة من الزمن. والمفتاح هو تابع رياضي يحوّل النص البسيط إلى نص مبعثر أو نص مشفر، ثم يعيد النص المشفر إلى نص بسيط. يمكن أن يختلف طول المفاتيح، من 40 بت إلى 2048 بت وأكثر من ذلك. بشكل عام، كلما ازداد طول المفتاح، يصعب على الكمبيوتر أن يفكك تشفير الرسائل المشفرة باستخدام جميع التركيبات الممكنة للحروف والأرقام. على كل حال، تحتاج المفاتيح الأطول إلى مزيد من المعالجة لتشغيل توابع التشفير وفك التشفير، لذلك يتم المقايضة باستخدام المفاتيح الأقصر لتحسين سرعة التشغيل. كما أن بعض البرامج التي تستخدم المفاتيح القصيرة تغيرها بشكل متكرر (مثلاً كل دقيقة) لذلك فإذا كسر المهاجم أحد المفاتيح، يجب أن يبدأ من جديد عندما يبدأ تشغيل المفتاح الجديد.

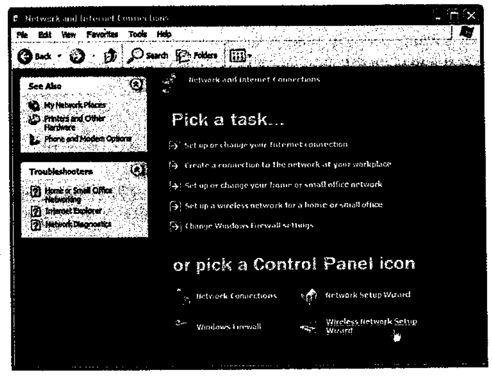
بما أن WEP استخدمت مفتاح قصير لفترة طويلة، ونفذت المفتاح أيضاً بشكل ضعيف، فقد اكتشف الباحثون سريعاً أنه بقليل من الوقت وبعض المساعدة من كمبيوتر، يستطيع المهاجم أن يفكك تشفير الإرسال المشفر مع WEP. ظهرت أدوات برمجية على الإنترنت بسرعة لتهاجم WLAN. وتستطيع الأداة الأكثر شهرة، التي تدعى AirSnort، أن تكسر الاتصالات المحمية بالمفتاح WEP في دقائق.

تواجه الآليتان WAP وWPA2 نقاط ضعف الآلية WEP باستخدام مفاتيح أطول وتغيير هذه المفاتيح بتردد أكبر. إذا كنت تشتري نقطة وصول لاسلكية في هذه الأيام، فإنها

تستخدم WAP أو WPA2؛ قد تحتاج أجهزة WLAN الأقدم إلى ترقية برمجياتها من WEP إلى WPA. على كل حال، إذا لم تتوفر الترقية المطلوبة، يجب أن تستمر باستخدام WEP، لأن بعض الحماية أفضل من لا شيء. (المفتاح WEP عديم الفائدة لشبكات الشركات، التي يتم استهدافها من المجرمين وتملك الكثير من المعلومات الحساسة التي تعبر الشبكة اللاسلكية، على كل حال، WEP كاف لمنع جارك من التطفل على شبكتك).

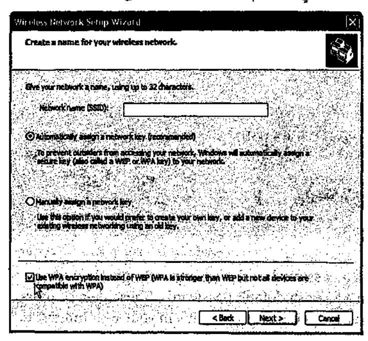
تقدم الآليتان WPA وWPA2 أنماطاً مختلفة للمستخدمين المنـزليين والأعمال. يجب أن يحدد المستخدمون المنـزليون الخيار WPA-PSK (المفتاح المشارك للوصول المحمي Wi-Fi) عند إعداد نقطة وصول لاسلكية. يحتاج WPA-PSK لإعداد جملة مرور تستخدمها نقطة الوصول لتوليد مفتاح تشفير. تستخدم جملة المرور الجيدة الأرقام والحروف. وتدخل هذه الجملة في كل جهاز تريده أن يتصل بنقطة الوصول. وبعد تشغيل WPA، يتم تشفير جميع الاتصالات بين الكمبيوتر ونقطة الوصول.

يقدم ويندوز XP سرفيس باك 2 (SP2) معالج إعداد شبكة لاسلكية لمساعدتك بإعداد شبكة WLAN. لكي تجد المعالج، انقر Start، ثم اختر Control panel و Network and Internet Connections. فترى معالج إعداد الشبكة اللاسلكية إلى جانب رمز البطاقة اللاسلكية، كما هو مبين في الشكل 9-1.



الشكل (9-1): الوصول إلى معالج إعداد الشبكة اللاسلكية.

يقودك المعالج عبر جميع الخطوات الضرورية لإنشاء شبكة لاسلكية محمية. تطلب منـــك الشاشة الأولى أن تختار SSID (يتم نقاشه في القسم التالي)، كما هو مبين في الشـــكل 9-2. وتسألك فيما إذا كنت تريد أن تسند مفتاح شبكة بشكل تلقائي أو يدوي. وهو مفتاح تشفير يحمي اتصالاتك. توصي مايكروسوفت بالإعداد التلقائي. إذا كانت نقطة الوصـــول تـــدعم WPA، دقق المربع في أسفل الشاشة لكي تستخدم التشفير WPA، دقق المربـــع في أســـفل الشاشة لكي تستخدم التشفير WPA بدلاً من WEP.



الشكل (9-2): اختيار SSID وWPA.

بالإضافة إلى التشفير، توجد آلية أمنية أخرى للشبكات اللاسلكية. وهي 802.1x. وهي إطار العمل لإرسال معلومات التحقق من الصحة، مثل كلمات المرور، الشهادات الرقمية أو العلامات الأمنية، لتمنحك الوصول إلى الشبكة اللاسلكية. يجب أن لا تقلق بشـــأن 802.1x عند إعداد شبكة منـــزلية، لكنك قد تواجه هذا المعيار إذا اشتريت وقتاً على شبكة لاسلكية عمومية، كما في فندق أو مقهى.

يمكنك اتخاذ خطوات إضافية أيضاً لتحمي الشبكة Wi-Fi، التي سنغطيها في الأقســـام التالية.

تغيير SSID الافتراضي

محدد إعداد الخدمة SSID هو محدد 32 حرف لنقطة الوصول اللاسلكية. يتصرف المحدد SSID كاسم الشبكة لتفريق نقطة الوصول أو WLAN المستخدمة عـــن نقـــاط الوصـــول

الأخرى. يجب على أي جهاز يريد أن يتصل مع نقطة الوصول أن يعــرف المحــدد SSID. والمشكلة هي أن معظم الباعة يقدمون نقاط الوصول مع المحدد SSID الافتراضي نفسه (على سبيل المثال، "default"). وهذه المحددات المعدة في المصنع معروفة جيداً، لــذلك تحتــاج إلى تغييرها. يمكنك أن تختار أي اسم تفضله من أجل المحدد SSID. لكن المحدد الأفضل هو الذي يستخدم مجموعة من الكلمات والحروف. يتم إرسال المحددات عادةً في الهواء بدون تشــفير، لذلك يجب أن لا تستخدم معلومات حساسة مثل تاريخ ولادتك، كلمــات المــرور علــى الإنترنت، اسمك أو عنوانك.

وإذا غيّرت المحدد SSID على نقطة الوصول AP، سوف تحتاج إلى إدخال المحدد نفسه على أي كمبيوتر تريد أن تمنحه الوصول إلى AP.

إيقاف إذاعة SSID

قد تكون نقطة الوصول معدة لإذاعة المحدد SSID بفترات دورية (مثلاً كل بضع ثوان). وهذه الميزة مفيدة للشبكات WLAN الكبيرة عندما ينتقل المستخدمون من نقطة وصول إلى أخرى. لكن هذه الميزة غير ضرورية للشبكة المنــزلية، لذلك يجب أن تلغي تأهيلــها لتمنــع المتدخلين من معرفة اسم شبكتك.

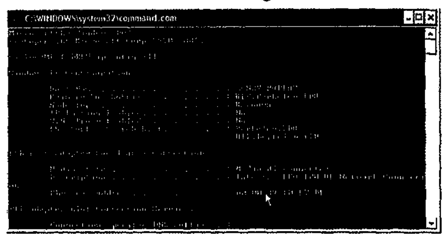
تغيير كلمات المرور الافتراضية

قد تطلب منك نقاط الوصول أن تختار كلمة مرور لتغيير أي إعداد. على كل حــال، كما مع المحددات SSID، فإن العديد من الباعة يسوقون نقاط الوصول مع كلمــات مــرور افتراضية. وكلمات المرور الافتراضية معروفة جيداً بالنسبة إلى المجرمين والمسيئين، لذلك مــن مصلحتك أن تغيرها.

تأهيل الترشيح MAC

تسمح بعض نقاط الوصول بإعداد AP فيتم السماح للكمبيوترات مع عناوين MAC محددة فقط بالوصول إليها. (لاحظ أن العنوان MAC لا علاقة له بالكمبيوترات ماكينتوش، التي تدعى Macs اختصاراً. إن MAC هي اختصار التحكم بالوصول إلى الوسائط). العنوان MAC هو رقم فريد يتم إسناده إلى كل بطاقة واجهة شبكة (NIC) – ولا يوجد بطاقتــان NIC تحتويان على الرقم نفسه. تدعى في بعض الأحيان NIC ببطاقة الأثيرنــت وتســتخدم لوصل الكمبيوترات إلى الشبكات. تتضمن معظم الكمبيوترات التي تم بيعها في السنين الأخيرة بطاقة NIC. وبما أن العناوين MAC فريدة، فإن ترشيح MAC هــو طريقــة فعالــة لمنــع الكمبيوترات غير المعروفة من استخدام شبكتك WLAN.

لكي تجد عنوانك MAC، انقر على الزر Start، حدد Run، واكتـــب command. فيفتح إطار DOS مع موجه وامض C. اكتب ipconfig/all إلى جانب الموجه C واضـــغط Enter. فيعرض الكمبيوتر لائحة بمواصفات الكمبيوتر، كما هو مبين في الشكل 9-3. ابحث عن الإدخال Physical Address، فيكون عنوانك MAC. يستخدم العنوان MAC الأرقام والحروف ويبدو كما في هذا العنوان 00.0D.60.FE.0f.1B. وإذا لم يملك كمبيوترك بطاقة NIC، لا يمكنك استخدام الترشيح MAC.



الشكل (9-3): عنوان الكمبيوتر MAC.

البرمجيات الأمنية اللاسلكية

إذا أهّلت WPA واتبعت خطوات تأمين الوصلة اللاسلكية الأخرى، سوف تكون على الأغلب أكثر أمناً من معظم الناس حولك. وهذا الأمر جيد لأن مجرمـــي الإنترنـــت يميلـــون لاستغلال الفرص: فيهاجمون الأهداف غير المحمية في البداية.

على كل حال، إذا أردت أمناً إضافياً، يمكنك أن تشتري برمجيات أمنيـــة لاســـلكية. وتكمن القيمة الحقيقية لهذه البرامج الإضافية في المساعدة التي تقدمها عندما تتصل بالشبكات اللاسلكية الأخرى، مثل مقهى أو فندق.

يقدم بائع البرمجيات الأمنية McAfee مسحاً مجانياً ليدقق أمن وصلة الشبكة اللاسلكية المستخدمة. يحمّل الاختبار تحكم أكتيف إكس إلى كمبيوترك لإجراء التدقيق، لذلك يجب أن تستخدم برنامج الاستعراض إنترنت إكسبلورر لبدء عملية التدقيق. لكي تشـــغّل الاختبـــار، اذهب إلى www.mcafee.com. انقر على قسم المستخدمين المنـــزليين وانظـــر إلى أســـفل القسم Free Services لكي تجد المسح McAfee Wi-Fi Scan.

وقد أضافت Trend Micro كشف التدخل Wi-Fi Intrusion Detection إلى PC-cillin الذي يضم أيضاً جدار نار شخصي، برمجيات مضادة للفيروسات، وبرمجيات مضـــادة

للسبايوير. تحذرك وحدة كشف التدخل Wi-Fi عند وجود حرب قيادة أو عنـــدما يـــدخل مستخدم إلى شبكتك اللاسلكية. اذهب إلى www.trendmicro.com.

تصنّع شركة تدعى OTO، Wi-Fi Defense 1.0، وهي برمجيات لمساعدتك على حماية الشبكة اللاسلكية. تؤهل تلقائياً الإعدادات الأمنية لشبكتك WLAN وتساعدك على مراقبة جميع المستخدمين الموجودين على شبكتك. كما تسهل إضافة المستخدمين أو إزالتـــهم مـــن شبكتك اللاسلكية اذهب إلى www.otosoftware.com.

وأصدرت Zone Labs البرمجيات الأمنية اللاسلكية ZoneAlarm. تكشـــف هـــذه البرمجيات الشبكات اللاسلكية تلقائياً وتساعد بحمايتها. كما تسمح باستخدام إعدادات أمنية مختلفة للشبكات اللاسلكية المختلفة التي تستخدمها بشكل عام. تضم البرمجيات أيضاً جدار نار ZoneAlarm. اذهب إلى www.zonelabs.com لمزيد من المعلومات.

وتقدم LucidLink برمجيات أمنية لاسلكية مجاناً لمساعدتك على إعداد شبكة المنـــزل اللاسلكية. يبسط هذا المنتج الخطوات الضرورية لإعداد نقطة وصول لاسلكية ولإضافة وإزالة المستخدمين من الشبكة WLAN. تبقى هذه البرمجيات مجانية لثلاثة مستخدمين كحد أقصى؛ على كل حال، تحتاج إلى استخدام كمبيوتر منفصل على الشبكة الموصولة ســـلكياً ليعمـــل كوحدة إدارة أمنية. يرخص هذا الكمبيوتر الموصول سلكياً الكمبيوترات اللاسلكية ليصلها مع الشبكة اللاسلكية. لمزيد من المعلومات اذهب إلى www.lucidlink.com.

3-9 أمن الأماكن العامة

إن الشبكات اللاسلكية غير مصممة للمنازل فقط. فالعديد من الأماكن العمومية، بمـــا في ذلك المقاهي، مطاعم الوجبات السريعة، الفنادق، ساحات البلدة، مخازن الكتب والمكتبات تقدم وصلات الشبكات اللاسلكية. تعكس هذه الشبكات WLAN العمومية الخدمة العظيمة التي يقدمها الوصل اللاسلكي. وبالفعل، فإن شركة تصنيع الطائرات بوينغ تبني الآن طائرات مجهزة بنقاط الوصول اللاسلكي. سوف تنقل هذه النقاط AP البيانات إلى هوائي اتصالات مع الأقمار الصنعية على الطائرة، والذي بدوره سيرسل البيانات إلى مجموعة من الأقمار الصـــنعية ويعيدها إلى المحطة الرئيسية على الأرض. ما هي النتيجة؟ المسافرون على الطائرة المجهزة جيداً سوف يتصلون بالإنترنت على ارتفاع 35000 قدم باستخدام الكمبيوترات المحمولة المؤهلـــة بالتقنية Wi-Fi القياسية (هذه الخدمة متوفرة حالياً على بعض الخطوط الجوية وعلى رحلات محددة، لكنها قد تصبح متوفرة على جميع الطائرات قريباً).

هناك طريقتان للبحث عن الشبكات اللاسلكية في الأماكن العامة. الطريقة الأولى هـــي بمراقبة الأطر المنبثقة على كمبيوترك المحمول عندما تكتشف رقاقة أو بطاقة شـــبكة لاســـلكية وجود شبكة لاسلكية. والطريقة الثانية، بمساعدة خدمات عديدة تساعد على البحـــث عـــن

الشبكات اللاسلكية في الأماكن العامة. تقدم إنتل برمجيات وطنية ودولية للبحث عن الشبكات اللاسلكية في الأماكن العامة في الموقع http://intel.jiwire.com. إذا كنت تفضل التجول على الإنترنت وأنت تشرب القهوة، يمكنك أن تبحث عن الأماكن العامة Starbucks في www.starbucks.com/retail/wireless.asp. هناك خيار جيد آخر في www.wiFinder.com، دليل عالمي للأماكن العامة مع الشبكات اللاسلكية 802.1b و802.11g.

تفرض بعض هذه الخدمات أجرة لقاء الوصول، ويجب أن توقع من أجل هذه الخدمة. على سبيل المثال، تكلف الخدمة T-Mobile HotSpot $29.99 في الشهر من أجل الوصول اللاسلكي غير المحدد في المواقع المشتركة، والتي تضم Starbucks، Borders وKinkos. ولكي تساعد في تأمين وصلتك، فإن الخدمة T-Mobile تستخدم 802.1x معيار أمني من أشخاص جيدين في IEEE. لاحظ أن 802.1x ليست معيار تشفير. إذا رأيت شبكة لاسلكية تستخدم 802.1x، يعني ذلك أنها تقدم بعض إجرائيات التحقق من الصحة فقط. ولكي تشفر البيانات، تحتاج أيضاً إلى استخدام WPA أو SSL. (تعني SSL طبقة المقابس المحمية. وهذا البروتوكول الذي يؤهل الإرسال المشفر للمعلومات عبر الوب). تستخدم الخدمة T-Mobile طبقة المقابس المحمية SSL.

لاحظ أن نظام التشغيل ويندوز XP يملك دعماً مبيتاً للمعيار 802.1x؛ ويجب أن يكون مؤهلاً بشكل افتراضي. يمكنك أن تدقق فيما إذا كان 802.1x مؤهلاً على كمبيوترك بالذهاب إلى www.microsoft.com وكتابة Set up 802.1x anthentication في حقل البحث. يعيد البحث عدة ارتباطات تشرح تعليمات عن تأهيل 802.1x.

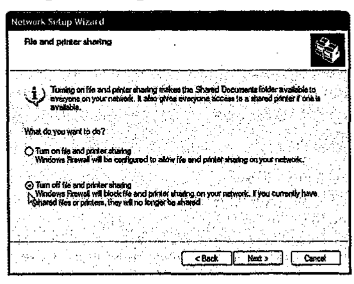
الشبكات اللاسلكية غير المحمية في الأماكن العامة

إن الخطر الكبير الذي يتعرض له مستخدمي Wi-Fi يأتي من الأماكن العامة التي لا تستخدم أي من وسائل التشفير المبنية في نقاط الوصول اللاسلكية. وتقبل هذه الشبكات غير محمية أي شخص يريد الانضمام إليها، وتكون الميزات الأمنية غير مؤهلة لتسهيل وصول المستخدمين. على كل حال، يعني ذلك أن برمجيات التجسس يمكنها تجميع المعلومات الحساسة.

إذا كنت تستخدم شبكة لاسلكية عامة مجانية، يجب أن تتخذ خطوات لتأمين الوصلة. تذكر أن كمبيوترك يتصرف كمحطة راديوية عندما تستخدم وصلة شبكة لاسلكية: كل البيانات التي تولدها يتم إذاعتها على جميع المستخدمين الموجودين في مجال الاستقبال.

إن العديد من هذه الخطوات هي من أفضل الإجراءات الأمنية العامة، مثل ضمان عمل جدار النار والبرمجيات المضادة للفيروسات (انظر إلى الفصل الثالث، "جدران النار"، والفصل

الرابع، "التخلص من الضيوف غير المرغوبين، الجزء 1: الفيروسات والديدان"، لمزيد من المعلومات). يجب أن تلغي تأهيل مشاركة الملفات أيضاً لتمنع برمجيات التجسس من الوصول إلى مستنداتك عبر الإنترنت. تكون خدمة مشاركة الملفات والطابعات في ويندوز XP سيرفس باك 2 غير مؤهلة بشكل افتراضي. يمكنك أن تتأكد من ذلك بنقر الزر Start ثم تحديد Control panel وNetwork and Internet Connections. ثم انقر Network Setup Wizard (انظر إلى الشكل 9-1). يجب أن تنقر على العديد من الأسئلة حتى تصل إلى الشاشة التي تسألك عن تأهيل مشاركة الملفات والطابعات كما هو مبين في الشكل 9-4. إذا كانت مشاركة الملفات والطابعات مؤهلة، ألغ تدقيق هذا المربع.



الشكل (9-4): إلغاء تأهيل مشاركة الملفات والطابعات.

إذا كانت خدمة الشبكة اللاسلكية العامة غير مزودة بالإعدادات الأمنية WEP أو WPA، يمكنك أن تحمي بياناتك بالشبكة الخاصة التخيلية (VPN). تشفر الشبكات VPN البيانات المرسلة بين نقطتين؛ مثل جداري نار في طرفين متقابلين في الشركة أو من كمبيوتر محمول إلى شبكة الشركة. لقد تم إنشاء الشبكات VPN لحماية بيانات الشركة التي تنتقل عبر شبكة الإنترنت العامة من المتجسسين المرتبطين سلكياً؛ وهي مستخدمة على نطاق واسع في هذه الأيام. وبتشفير وصلتك اللاسلكية، تحمي نفسك من المهاجمين الذين يستخدمون أدوات التجسس اللاسلكية.

إذا كنت تستخدم كمبيوتر محمول في الشركة مع مستضاف VPN مثبت، يمكنك أن تستخدم VPN لكي تحمي وصلتك اللاسلكية من الشبكة اللاسلكية غير المحمية المستخدمة في مكان عام. وإذا لم يكن لديك مستضاف VPN من الشركة، يمكنك أن توقّع من أجل HotSpotVPN (www.hotspotVPN.com)، خدمة من شركة تدعى Wi-Fi Consulting.

تبدأ الأسعار من 10.88$ في الشهر. ويمكنك أن تحصل على اشتراك ليوم واحد، ثلاثة أيام، وسبعة أيام بدءاً من 3.88$.

هجوم التوأم البغيض

هناك خطر آخر في الشبكات اللاسلكية في الأماكن العامة وهو هجوم التوأم البغيض Evil Twin. يعمل هذا الهجوم كالتالي: يضع المهاجم كمبيوتر محمول في قرب شبكة لاسلكية في مكان عام. ثم يصل الكمبيوتر المحمول إلى نقطة وصول لاسلكية ويعطيه اسم الشبكة نفسه (المحدد SSSP) نفسه مثل نقطة الوصول النظامية. إذا كانت إشارة نقطة الوصول قوية بشكل كاف (أو إذا أعاق المهاجم نقطة الوصول النظامية)، يقدم التوأم البغيض نفسه كشبكة لاسلكية للمستخدمين الآخرين. وقد يعرض لهم شاشة تسجيل دخول قد تسأل عن رقم بطاقة الاعتماد. فإذا سجل المستخدمون الدخول في نقطة الوصول المخادعة، يسرق المهاجم هذه المعلومات المهمة التي يكشف المستخدم عنها على الإنترنت.

توجد عدة طرق جيدة للدفاع ضد هجوم التوأم البغيض. الطريقة الأولى هي إعداد البرمجيات اللاسلكية لكي لا تتصل تلقائياً بالشبكة الأقرب. وهناك حل أفضل بتأهيل المزايا الأمنية المبيتة في التقنية Wi-Fi (بافتراض أن الإعدادات الأمنية للشبكة اللاسلكية في المكان العام مؤهلة). يمكنك أن تستخدم أيضاً VPN، كما تم شرحه.

لاحظ أنه لم يتم التصريح عن عمليات هجوم بغيض كثيرة، لكن من المهم أن تعرف بوجود التهديدات الكبيرة لكي تأخذ الإجراءات المناسبة بشكل مسبق.

لا تنفذ معاملات حساسة على شبكة لاسلكية في مكان عام

إن الخيار الأفضل أمنياً هو عدم إجراء المعاملات المصرفية ومعاملات التجارة الإلكترونية على الوب عبر شبكة لاسلكية في مكان عام. فتتقي بذلك من خطر التعرض إلى هجوم التوأم البغيض أو إلى محاولة أخرى لسرقة المعلومات الحساسة من البيانات المرسلة لاسلكياً.

4-9 أمن الهاتف الخليوي وPDA

إن الهواتف الخليوية، المساعدات الرقمية الشخصية PDA وأجهزة البريد الإلكتروني اللاسلكية هي أدوات مناسبة للاتصال والأعمال، وهي تقدم مجموعات مختلفة من المزايا والإمكانيات. يمكنك أن تشتري PDA يضم هاتف خليوي وإمكانية إرسال واستقبال البريد الإلكتروني، ويمكنك أن تشتري هاتف خليوي مع مزايا مثل استعراض الوب، الوصول إلى البريد الإلكتروني، التقويم، كاميرا رقمية والرسائل النصية (تدعى هذه الهواتف الخليوية بالهواتف الذكية). يمكن أن تستخدم الهواتف الخليوية وPDA أيضاً Wi-Fi أو بلوتوث لكي تتصل مع

الأجهزة الخليوية الأخرى، الكمبيوترات النظامية والشبكات اللاسلكية.

ومع اندماج هذه الأدوات في الطريقة التي نعمل ونتسوق بها، تصـــبح أيضـــاً أهـــدافاً للمسيئين والمجرمين. قد يطلق الأشخاص الممازحون هجوماً مزعجاً لإعاقة الخدمة أو استجرار طاقة بطاريات الجهاز. على كل حال، قد تصبح الهواتف الخليوية والمساعدات PDA أهـــدافاً لهجوم التصيد وعمليات الخداع الأخرى التي تبغي السرقة.

في الوقت الحالي، ما تزال الأجهزة الخليوية بعيدة نسبياً عن الإصابة بـــبرامج المـــالوير بالمقارنة مع الأجزاء المقابلة من الكمبيوترات. على كل حال، بـــدأت الأجهـــزة الخليويـــة باستخدام عدة أنظمة تشغيل عامة ووسائل اتصال، تسهل انتشار برامج المالوير. وبالفعل، لقد ظهرت عدد من فيروسات الهواتف الخليوية والمساعدات PDA. ولكن معظمها ما زال محدود الانتشار وبدون أي مضمون خبيث.

سوف نبحث في مبادئ أنظمة التشغيل الجوالة ووسائل الاتصال التي تستخدمها برامج المالوير غالباً كوسيلة لانتشارها.

أنظمة التشغيل الجوالة وبلوتوث

إن معظم الأجهزة الجوالة تعمل على نظامي تشـــغيل PalmOS و Microsoft Windows Mobile (دعي سابقاً Pocket PC). وبدأت الهواتف الخليوية باســـتخدام نظـــام التشـــغيل Symbiam (OS)، وهو اتحاد بائعي الهواتف الخليوية، لقد تم تطوير Symbian جزئياً لكـــي يمنع سيطرة مايكروسوفت على عالم الهواتف الخليوية. وكما تم نقاشه في الفصل الرابع، فـــإن انتشار المالوير هو عملية أسهل عندما يكون عدد أنظمة التشغيل قليل وعدد الأجهزة كـــبير. وهذا الأمر لا بد منه كنتيجة للمعايير وشروط العمل المتبادل.

يجب أن تعرف أيضاً عن بلوتوث، وهي تقنية لاسلكية قصيرة المجال (حوالي 10 أمتار أو 32 قدم) تسمح بوصل الأجهزة المنفردة لتشكل شبكات مناطقية شخصية (PAN). يمكن أن تستخدم الهواتف الخليوية، المساعدات PDA، والكمبيوترات المحمولة بلوتوث لكي تتصل مع بعضها وتنقل المعلومات الرقمية، بما في ذلك الملفات. يتم استخدام بلوتوث في فأرة الكمبيوتر، لوحة المفاتيح، والمجموعة الصوتية الرأسية. بالإضافة إلى ذلك، تستخدم بعض السيارات تقنية بلوتوث لكي تسمح باستخدام الهواتف بدون مسكها باليد.

يتم مراقبة التقنية بلوتوث من مجموعة الاهتمامات الخاصة بلوتـــوث (SIG). وقـــد تم تأسيس بلوتوث SIG من شركات تقنية مشهورة تشمل Nokia، Intel وIBM. وتدعم حالياً آلاف من الشركات الأعضاء. وبينما توفر بلوتوث حلاً ملائماً لربط المنتجات المنفصلة، يحتمل أن تصبح وسيلة شائعة لإصابة الأجهزة الجوالة ببرامج المالوير.

مالوير الهواتف الخليوية

لقد ظهرت عدة أنواع من المالوير استهدفت الهواتف الذكية. سوف ننظر إلى أربعة أمثلة ثم نناقش طرق الحماية من هذه البرامج وغيرها من برامج الهواتف الذكية.

- ظهرت الدودة Cabir في حزيران 2004. استهدفت نظام تشغيل الهاتف الجوال Symbian واستخدمت بلوتوث لكي تنتشر إلى الأجهزة الأخرى. طلبت الدودة من المستخدمين أن يوافقوا على استقبال رسالة. إذا قبل المستخدم باستقبال الرسالة، يتم توجيهه لتثبيت ملف. ومن يقوم بتثبيت الملف يصاب بالدودة. ومع أن هذه الدودة لا تملك أي وظيفة خبيثة، لكن الهواتف المصابة عانت من نقص زمن حياة البطارية لأن الدودة تبحث باستمرار عن الأجهزة المؤهلة بالتقنية بلوتوث الأخرى.
- ظهر حصان طروادة Skulls في تشرين الثاني 2004، واستهدف Symbian OS. ولكي يتم التقاط حصان طروادة، يجب على المستخدمين أن يحملوا برنامج يظهر كأداة برمجية لإدارة المواضيع على الهاتف الذكي Nokia 7610. إذا حمّل المستخدم البرنامج، يدعى Extended Theme.SIS (تعني SIS نظام تثبيت Symbian)، يتم استبدال جميع رموز التطبيقات بصورة الجمجمة والعظمتين المتصالبتين. يستطيع المستخدمون المصابون بحصان طروادة المذكور أن يتابعوا في إجراء المكالمات الصادرة وقبول المكالمات الواردة، ولكن يتم إلغاء تأهيل جميع التطبيقات الأخرى. وقد تم إضافة الدودة Cabair إلى بعض الإصدارات من حصان طروادة المذكور.
- في كانون الثاني 2005، اكتشف باحثو الفيروسات الدودة Lasco A، التي استهدفت Symbian OS عبر بلوتوث وإذا تشارك المستخدمين بملفات SIS مصابة. يجب على المستخدمين أن يوافقوا لكي يثبتوا الملف الذي يحتوي على الدودة. لقد كانت شيفرة المصدر للدودة Lasco مشابهة لشيفرة المصدر للدودة Cabir.
- استهدفت الدودة Mabir أيضاً Symbian OS واستخدمت بلوتوث لكي تنتشر. على كل حال، الأمر المميز في هذه الدودة هو إمكانية إرسال الملفات المصابة باستخدام الخدمة MMS، تعني خدمة رسائل الوسائط المتعددة، وهي مستخدمة لإرسال المواد الرقمية مثل الصور والملفات الصوتية. وبدأت الخدمات المصابة تبحث عن أهداف أخرى ضمن نطاق البلوتوث.

لم تعاني الهواتف الخليوية من هجمة كبيرة – وكان تأثير برامج المالوير المذكورة منخفضاً جداً. أي أنه من الواضح أنه توجد الخبرة الضرورية لكتابة فيروسات الهواتف الخليوية. وكل ما يتبقى لبدء عملية هجوم هي التوفيق بين البرمجيات والهندسة الاجتماعية. لذلك كما يقوم

الشخص الحكيم بسد الثقب في السقف في يوم مشمس بدلاً من انتظار هطول المطر، يجب أن يأخذ معظم مستخدمي الهواتف الذكية خطوات لحماية أنفسهم قبـــل أن يصـــدر مـــبرمج فيروسات محظوظ برنامجاً يتعمد الإصابة على نطاق واسع.

يبين الجدول 9-2 أن العديد من الشركات المشهورة المضادة للفيروسات أصدرت برمجيـــات مضادة للفيروسات من أجل الهواتف الخليوية (يتضـــمن Symantec Mobile Security 4.0 جدار نار أيضاً). تحميك البرمجيات المضادة للفيروسات من الفيروسات المعروفة. فإذا كان هناك برنامج استعراض في هاتفك الخليوي، يمكن أن تحمّل البرمجيات AV مباشرة إلى الهاتف. وإلا، يمكنك تحميل البرمجيات AV إلى كمبيوترك ونقلها عبر وصلة كابل أو بلوتوث. في منتصـــف 2005 كانت الأسعار تتراوح من 15.95$ إلى 44.96$. كما أن العروض الخاصة والمساومات تؤثر على السعر النهائي.

تأمين بلوتوث

كما يمكنك الاستدلال من برامج المالوير المشروحة، فإن تقنية البلوتوث هي ناقل محتمل لبرامج مالوير الهواتف الذكية. تسمح الأجهزة المؤهلة ببلوتوث باختيار مستويات أمنية أعلى أو أخفض. يشرح هذا القسم مختلف الإعدادات الأمنية، ولكن يجب أن تراجع دليل المستخدم من أجل إجراء التعديلات.

إذا لم تكن تستخدم بلوتوث، فإن الخيار الأبســـط والأكثـــر أمنـــاً هـــو إلغـــاء تأهيلها.

إذا استخدمت بلوتوث، يمكنك أن تعين مرئية الهاتف الذكي على النمط Hidden مخفي أو غير قابل للاكتشاف. فيمنع ذلك أي جهاز مصاب موجود ضمن المجال من إرسال برامج المالوير إليك. انظر إلى دليل الجهاز المزود ببلوتوث لتعرف طريقة تعيين هـــذه الميـــزة علـــى Hidden.

تسمح بلوتوث أيضاً بإنشاء أزواج أمنية بين أجهزة بلوتوث، مثل الهـــاتف الخليـــوي والمجموعة الرأسية. يشفر الزوج الأمني جميع الاتصالات بين جهازين. على كل حال، يجب أن تحذر من إنشاء الأزواج مع الأجهزة غير الموثوقة. وإذا أنشأت زوجاً، فاســـتخدم الإعـــداد Unauthorized؛ يضمن ذلك ترخيص أي طلب وصلة.

أخيراً، إذا كان لديك جهاز بلوتوث، احترس من قبول الملفات أو التطبيقات غـــير المطلوبة. وإذا استقبلت ملفاً عندما لا تتوقع ذلك، فإن الخيار الآمن هـــو أن ترفضـــه أو تحذفه.

الجدول (9-2):

البرمجيات المضادة للفيروسات للهواتف الخليوية والمساعدات PDA				
المنتج	البائع	منصة العمل	نظام التشغيل	موقع الوب
F-Secure Anti-Virus من أجل Pocket PC	F-Secure	PDA	Windows Mobile, Windows Pocket PC	www.f-secure.com
F-Secure Mobile Anti-Virus	F-Secure	مختلف الهواتف الخليوية، Nokia، N-Gage، SiemensSX1	Symbian OS	www.f-secure.com
Kaspersky AntiVirus Personal	Kaspersky Lab	PDA	PalmOS, Windows Pocket PC	www.kaspersky.com
PC-cillin من أجل الاتصال اللاسلكي	Trend Micro	PDA	PalmOS, Windows Pocket PC	www.trendmicro.com
Symantec AntiVirus من أجل الأجهزة المحمولة	Symantec	PDA	PalmOS, Windows Mobile, Pocket PC	www.symantec.com
Symantec Mobile Security 4.0	Symantec	الهواتف الذكية	Symbian OS	www.symantec.com
Trend Micro Mobile Security	Trend Micro	الهواتف الذكية	Windows Mobile من أجل Pocket PC Phone edition، Windows Mobile من أجل Smartphones، Symbian OS	www.trendmicro.com

أمن PDA

أصبحت المساعدات PDA بشكل متزايد أهدافاً للمجرمين لأنها تحفظ المعلومات الحساسة غالباً، مثل الأسماء وأرقام الهواتف، PIN، أرقام الحسابات، وحتى أرقام الضمان الاجتماعي. تواجه المساعدات PDA التي تستخدم بلوتوث العديد من نقاط الخلل نفسها التي تعاني منها الهواتف الذكية، بما في ذلك انتشار المالوير. كما هو مبين في الجدول 9-2، تقدم العديد من الشركات برمجيات مضادة للفيروسات للأجهزة المحمولة باليد لأن بعض الفيروسات التي تصيب الهواتف الذكية يمكن أن تصيب PDA أيضاً.

ما يزال عدد برامج المالوير التي أصابت المساعدات PDA قليلاً. في آب 2004، اكتشف الباحثون حصـــان طـــروادة Brador، اســـتهدف نظـــام التشـــغيل Windows Mobile 2003/Pocket PC. ومع أن الباحثين أنشؤوا برنامج مالوير PDA في المختبر لإثبات المبـــدأ، لكن Brador كان المثال الأول عن برنامج مالوير حقيقي. يسمح حصان طروادة المـــذكور، عند تثبيته بشكل صحيح، أن يقوم المهاجم بتحميل الملفات من وإلى PDA. ومع أن معـــدل إصابة Brador منخفض جداً، لكنه بيّن أن مبرمجي المالوير يملكون القدرة والرغبة باستهداف الأجهزة المحمولة التي تعتمد على مايكروسوفت.

على كل حال، الخطر الأكبر الذي يواجهه مستخدمي PDA هو خطر فيزيائي ولـــيس تقني. وعلى الرغم من أن المساعدات PDA تضيع أو يتم سرقتها بسهولة، فإن الكـــثير مـــن المستخدمين لا يزعجون أنفسهم بإعداد كلمة مرور لحماية المعلومات الحساسة. وهكذا، فمن يسرق جهازك PDA سوف يصل إلى المعلومات الشخصية التي حفظتها على الجهاز. تأكد من استخدام كلمة المرور لحماية معلوماتك. اختر كلمة مرور من الحروف والأرقـــام؛ فيصـــعب بذلك على المجرم كسر كلمة المرور. يجب أن تحجم أيضاً عن حفظ المعلومات الحساسة مثـــل أرقام الحسابات أو رقم الضمان الاجتماعي على الجهاز. وإذا احتجت إلى حفظ مثل هـــذه المعلومات على الجهاز، يمكنك استخدام برنامج التشفير المتوفر للأجهزة PDA لتأمين طبقـــة أمنية إضافية من أجل حماية البيانات.

5-9 أمن VoIP

إن بروتوكول الصوت عبر الإنترنت (VoIP) هو تقنية جيدة لإجراء الاتصالات الهاتفية عبر الإنترنت تعد الاتصالات الهاتفية التقليدية دارة مخصصة بين هاتفين، ويتم إرسال صـــوت مضخم الصوت كإشارة رقمية عبر هذه الدارة. وبالمقابل، فـــإن VoIP لا يحتـــاج إلى دارة مخصصة بين المتصلين. بدلاً من ذلك، يأخذ الصوت الصادر عن مضخم الصوت ويقسمه إلى رزم منفردة يتم توجيهها عبر شبكة الإنترنت العمومية بالطريقة نفسها كالبريد الإلكتـــروني وبيانات الوب. (لمزيد من المعلومات عن طريقة عمل IP، انظر إلى الفصل الثالث).

تقدم العديد من الشركات بما في ذلك Vonage، Packet 8، Verizon وSBS العديد من الحلول VoIP إلى المستهلكين وبكلفة أقل من خدمة الهاتف العادي. لا تحتاج هذه الخدمة VoIP إلا لشراء مهايئ خاص، تصل إليه خط الهاتف ووصلة الإنترنت عريضة المجـــال (أي كابل أو DSL).

هناك خيار آخر هو البرمجيات Skype (www.skype.com)، التي تسمح لك بإجراء مكالمات هاتفية مجانية من كمبيوترك إلى مستخدمي Skype الآخرين. يعمل Skype علـــى ويندوز، ماكينتوش ولينوكس. وكل ما تحتاج إليه هو مجموعة رأسية مع ميكروفون يمكنك أن

تصلها إلى كمبيوترك ووصلة الإنترنت. لقد تم تحميل Skype أكثر من 108 مليون مرة حتى الآن. وتقدم Skype أيضاً خدمة مدفوعة تدعى SkypeOut تسمح لك بإجراء الاتصالات من كمبيوترك إلى الهواتف العادية.

على الرغم من أن VoIP تمثل طريقة غير مكلفة لإجراء الاتصالات الهاتفية، لكنها تعاني من عدة أمور أمنية مهمة. أولاً، تحتاج إلى فتح مجال عريض من المنافذ الصادرة ومجال أصغر من المنافذ الواردة على جدار النار. وقد يحاول المهاجمون أو برامج المالوير المؤتمتة استغلال هذه المنافذ من أجل الوصول إلى كمبيوترك. في هذه المرحلة لا توجد تقارير عن محاولات واسعة الانتشار لاستغلال المنافذ المفتوحة لـ VoIP، ولكن مع ازدياد عدد المستخدمين الذين يوقعون من أجل هذه الخدمة، سيزداد احتمال وقوع هذه المحاولات. وبما أن VoIP يعتمد أيضاً على وصلة الإنترنت، فإن أي هجوم ضد هذه الوصلة قد يقطع الخدمة الهاتفية VoIP. بالإضافة إلى ذلك إذا كان مزود خدمة الإنترنت يعاني من أي نوع من الانقطاع (على سبيل المثال، انقطاع التغذية أو انقطاع الخدمة بسبب هجوم رفض الخدمة)، فسوف تتأثر الخدمة الهاتفية VoIP.

VoIP و911

هناك مسألة أكثر أهمية مع VoIP تتعلق بالمكالمات الطارئة 911. عندما تتصل بالرقم 911 باستخدام نظام الهاتف التقليدي، يتم الارتباط تلقائياً بين رقم هاتفك مع اسمك وعنوانك ويتم تقديم هذه المعلومات إلى مرسل الطوارئ في نقطة تأمين الخدمة العامة المناسبة (PSAP).

وتكون النقطة الأولى في الاتصالات الهاتفية الطارئة هي PSAP، التي توجد غالباً في أقسام الشرطة أو في وحدات إطفاء الحريق، مع أنه في بعض الحالات قد ترسل PSAP اتصال الطوارئ إلى وكالة الحماية المناسبة. وبما أن الخدمة الهاتفية التقليدية تعرض الاسم والعنوان إلى المرسل، يمكن إرسال وحدات الطوارئ حتى لو كان المتصل غير قادر على تقديم المعلومات.

على كل حال، بما أن التقنية VoIP تتجاوز الشبكة الهاتفية التقليدية، لا يتم ربط اسمك وعنوانك بشكل تلقائي إلى رقمك الهاتفي وتقديمها إلى مرسل الطوارئ. بالفعل، بعض خدمات المستهلكين VoIP لا تملك خدمة الاتصال 911 مؤهلة بشكل تلقائي. بل يجب أن تؤهل هذه الميزة يدوياً، وفي بعض الحالات يجب أن تدفع كلفة إضافية لقاء الخدمة. انظر إلى مستندات المستخدم لكي تعرف كيف تؤهل الاتصال 911 على الخدمة VoIP.

بالإضافة إلى ذلك، يجب أن تسجل موقعك على مزود الخدمة VoIP لكي يستطيع المزود أن يوجّه اتصالاتك إلى PSAP المناسبة. وإذا قدمت عنواناً غير صحيحاً أو إذا استخدمت الخدمة VoIP في موقع مختلف عما هو مذكور مع مزودك، لن يتم توجيه اتصالك VoIP 911 إلى PSAP الصحيحة.

لاحظ أيضاً أنه قد يتوجب عليك أن تخبر مرسل الطوارئ عن اسمك، رقـــم الهـــاتف، والعنوان إذا كنت تستخدم الاتصال 911 VoIP. وذلك لأن بعض أنظمة الاتصـــال VoIP توجه اتصالك إلى رقم PSAP عام، وليس إلى مركز متابعة الطوارئ.

أخيراً وكما ذكرنا، لن يعمل مزود الخدمة VoIP أثناء انقطاع التغذية، وبالتالي حتى لو أهلت الاتصال 911، لن تستطيع أن تجري أو تستقبل أي اتصال هاتفي VoIP.

تطور لجنة الاتصالات الفيدرالية خططاً لإلزام جميع المزودات VoIP بتـــوفير إمكانيـــة الاتصال 911. وبالإضافة إلى ذلك، تعمل المزودات VoIP لتزويد إمكانيات الاتصـــال 911 تلقائياً. على كل حال، إذا استخدمت VoIP في الوقت الحالي قد تضطر إلى تأهيل اتصـــال الطوارئ 911 يدوياً.

6-9 لائحة التدقيق

استخدم هذه اللائحة كدليل مرجعي للمواد المغطاة في هذا الفصل.

ما يجب أن تفعله

- تذكر أن الشبكات اللاسلكية ترسل الإشارات الراديوية التي يمكن أن تلتقطهـــا أجهـــزة الكمبيوتر اللاسلكية الأخرى.
- تأهيل WEP أو WPA لكي تشفر البيانات اللاســـلكية، ولتضـــمن أن المســـتخدمين المرخصين فقط يصلون إلى نقطة الوصول.
- اتخاذ خطوات إضافية لحماية شبكتك اللاسلكية، بما في ذلك تغيير SSID.
- استخدام جدار نار، وإلغاء تأهيـــل مشـــاركة الملفـــات عنـــدما تكـــون في الأمـــاكن العامة.
- استخدام البرمجيات المضادة للفيروسات على البطاقة الهاتفية الذكية وPDA.
- استخدام كلمة المرور لتحمي المعلومات على DA} إذا تم سرقتها.
- تأهيل الاتصال 911 إذا كنت تستخدم VoIP.

ما يجب أن لا تفعله

- استخدام SSID أو كلمات المرور الافتراضية عند إعداد الشبكة اللاسلكية.
- إجراء المعاملات الحساسة مثل المعاملات المصرفية على الوب أو الشراء على مواقع التجارة الإلكترونية في الأماكن العامة.
- نسيان أن تؤهل الاتصال 911 إذا كنت تستخدم VoIP.

7-9 موارد مساعدة

يقدم هذا القسم موارد إضافية لمساعدتك على تعلم المزيد.

إذا كنت تبحث عن مزيد من المعلومات عن التقنية والمنتجات Wi-Fi، تجد كثير من المعلومات الرائعة في كوكب Wi-Fi، www.wi-fiplanet.com. يقدم هذا الموقع دورات تعليمية، تقارير عن المنتجات، معلومات أمنية وأكثر من ذلك.

يمكنك أن تجد مخططاً مساعداً يقدم مزيد من المعلومات عن 802.11b، g، والمعايير اللاسلكية في www.linksys.com/edu/wirelessstandards.asp.

تقدم مايكروسوفت معلومات عن الشبكات اللاسلكية وأمنها، بما في ذلك توصيات للمحافظة على الأمن في الأماكن العامة. اذهب إلى www.microsoft.com/atwork/stayconnected/hotspots.mspx.

وتقدم إنتل توصيات عن أمن الشبكات اللاسلكية في www.intel.com/personal/do-more/wireless/security/.

الفصل العاشر

الخصوصية والإنترنت

إننا نعيش في عصر يقوم على تجميع وتحليل البيانات. والشبكات الإلكترونية التي تشكل دعامة تجارتنا واتصالاتنا تؤهل أيضاً عمليات غير مسبوقة لتجميع وحفظ ومشاركة (أو بيع) المعلومات الشخصية. وتدفع قوتان محرك التجميع المذكور، الأولى تجارية والأخرى حكومية. ولكل قوة دوافعها ومواردها (على الرغم أنه في العديد من الحالات تتقارب هذه المـوارد)، لكنهما يعتمدان على مصدر واحد: أنت وأنا.

في الحقل التجاري، يكدس سماسرة البيانات قواعد البيانات بمعلومات مهمة مثل رقـم الضمان الاجتماعي، تاريخ الولادة، الحالة العائلية، والدفعات الشهرية، بالإضافة إلى المعلومات غير المهمة مثل أفضلياتك في اختيار معجون الأسنان. يتم تجميع هذه البيانات وبيعها لجهـات مختلفة. وبدورها تحلل هذه الجهات البيانات على أمل الحصول على معلومات مفيدة. هل لدى طالب العمل سجل إجرامي؟ هل يهتم هذا المستهلك بتلقي معلومات عن شركة جديدة لإنتاج معجون الأسنان؟

وعلى الجانب الحكومي هناك تقليد استخباراتي قديم بتجميع المعلومات الدولية والمحليـة من أقسام الشرطة ووكالات التجسس. يتم استخدام هذه المعلومات الاسـتخبارية لتحقيـق أهداف في السلك الدبلوماسي، التجاري، محاربة الجريمة، الحرب والأمن القـومي. وطـوال خمسين سنة ماضية تم تعبئة الموارد الحكومية ببنية تحتية من المعلومات المجمعة من أجل الحـرب الباردة. أما في هذه الأيام فإن الدافع الأكبر لتجميع البيانات على نطاق واسع هـو محاربـة الإرهاب.

وعلى الأغلب فإننا نحن المواطنون نستفيد من الحركة التجاريـة والحكوميـة لتجميـع المعلومات. فيسهل سماسرة البيانات الأمر علينا بتسهيل أخذ القروض، شراء منـزل أو تأجير منـزل، العلم بحدوث أي نشاط غريب على بطاقة الاعتماد وهكذا. وتؤهلنا أيضاً للاستفادة من المنافسات التجارية (مثل الحصول على بطاقة تخفيض لشركة معجون أسنان أخرى) وتعاون

الشركات (كالحصول على سفرات جوية عند شراء بطاقة اعتماد). وأثناء ذلك تتعقب وتشارك الوكالات المحلية والفيدرالية بالمعلومات لتقبض على المجرمين وتحارب الخداع. تأمل الحكومة أيضاً بأن هذه المعلومات التي يتم تجميعها من أقسام الشرطة ووكالات محاربة الإرهاب ستمنع تكرار هجمات كهجوم 9/11.

لكن هناك جانب غامض لعملية تجميع المعلومات الهائلة، يجلب إلى الأذهان أفكار المؤامرات التي تنفذ أعمال عالمية أو سيناريوهات المراقبة الموجودة في كل مكان والتي ترصد جميع الحركات. المشكلة هي أن هذه السيناريوهات تحتوي على بعض من الحقيقة. تحدث الفصل الثاني، "منع سرقة الهوية" باختصار عن فضيحة ChoicePoint، والتي أعلن فيها سمسار البيانات ChoicePoint أنه باع معلومات شخصية حساسة لحوالي 145000 شخص إلى سارقي الهويات لكي يستخدموها كأصحاب عمل نظاميين. لقد كشفت هذه الفضيحة أمام الأميركيين حجم المعلومات الشخصية التي يتم تجميعها - وحجم الأموال التي يتم الحصول عليها من بيع هذه المعلومات. ويشير محامو الخصوصية إلى أنظمة تجميع البيانات المدعومة من الحكومة مثل Echelon (نظام مراقبة إلكتروني عالمي تديره بشكل جزئي وكالة الأمن القومي (NSA)) وCarnivore (برنامج يسمح لأقسام الشرطة في الولايات المتحدة التدقيق في البريد الإلكتروني واتصالات الإنترنت الأخرى). والحقيقة هي أن فوائد محرك البيانات تأتي لقاء ثمن: اضمحلال الخصوصية المتعلقة بعاداتنا، أفضلياتنا، ومعلوماتنا الشخصية، والاحتمال القائم بإساءة استخدام هذه المعلومات.

على سبيل المثال، يحاول سارقو الهوية بشكل دوري فتح أجهزة حفظ البيانات. ويتم إعاقة المواطنين الأبرياء عند ركوب الطائرات لأن أسماءهم موسومة بإرهابي ممنوع من الطيران على لوائح المراقبة. (وحتى الأشخاص المهمين غير محصنون ضد هذه الأخطاء. في عام 2004، تم حجز السيناتور تيد كينيدي، أحد أكثر السياسيين المعروفين في الولايات المتحدة، في المطار من أجل هذا السبب بالتحديد).

يمكن أن تسبب هذه المعلومات الخاطئة أيضاً تداعيات سياسية. في الانتخابات الرئاسية عام 2004، تم إبعاد مئات من الناخبين عن صناديق الاقتراع في فلوريدا لأنه ورد ذكرهم خطأً كمجرمين سابقين وأنهم لا يملكون الحق بالتصويت. وفي الحرب على الإرهاب، يتم احتجاز الأشخاص الأبرياء بدون تمثيل قانوني.

لسوء الحظ، خرج الجنّي من القارورة فيما يتعلق بتجميع البيانات. على كل حال، يمكنك أن تتخذ خطوات لتحصل على بعض الخصوصية، على الأقل على الوب. يختبر هذا الفصل الطرق المختلفة للتأكيد على حقوق الخصوصية على الإنترنت. وسوف نبين كيف تكشف عن المعلومات التي يتم تجميعها من سماسرة البيانات الرئيسيين.

1-10 خيارات خصوصية الإنترنت

من الممكن أن تحصل على مستوى مقبول من الخصوصية عند استخدام الإنترنت. تتوفر البرمجيات التي تشفر البريد الإلكتروني والرسائل الفورية التي ترسلها والملفات والمجلدات التي تحفظها على كمبيوترك. بالإضافة إلى ذلك، تساعد مقنّعات الوب على إخفاء هوية المواقع التي تزورها.

إن التشفير هو عملية يتم تطبيقها على المعلومات (التي تدعى بالنص البسيط) حيث يتم معالجتها بخوارزمية رياضية وتحويلها إلى نص مبهم (نص مشفر). والطريقة الوحيدة لإعادة النص المشفر إلى نص بسيط هي باستخدام مفتاح، وهو رمز سري يتم تطبيقه مع عملية رياضية أخرى لإعادة النص المشفر إلى نص بسيط. وكما تم نقاشه في العديد من الفصول الأخرى، فإن الإنترنت تعتمد على التشفير من أجل التجارة الإلكترونية ولكي تتحقق من صحة المتعاملين الذين ليس لديهم آلية لإقامة الثقة أو تبادل شهادات اعتماد الهوية في العالم الحقيقي.

مبادئ التشفير

يوجد بشكل عام نوعين من التشفير الرقمي: المتناظر وغير المتناظر. في التشفير المتناظر يتم استخدام المفتاح نفسه لتشفير النص البسيط وفك النص المشفر. يعتمد أمن التشفير بشكل جزئي على الخوارزمية المستخدمة وطول المفتاح. تدعى الخوارزمية القياسية. معيار التشفير المتقدم (AES). تدعم هذه الخوارزمية مفاتيح من مختلف الأطوال، ويقاس طول المفتاح بالبتات. ويتم الحكم على قوة المفتاح بالزمن اللازم لكمبيوتر متوفر تجارياً لتفكيك الرسالة المشفرة وذلك بتجريب جميع التراكيب الممكنة للحروف والأرقام. يدعى ذلك هجوم القوة الوحشية، وهي الطريقة المباشرة في كسر الشيفرة. على كل حال، تعطي هذه الطريقة قياساً جيداً، لأنه يجب أن تفترض أن عدوك يصل إلى تقنيات الكمبيوترات المتوفرة على نطاق واسع.

في هذه الأيام تعتبر المفاتيح 40 بت عديمة الفائدة؛ ويستخدم الحقل الصناعي مفاتيح بطول 128 بت، 250 بت و512 بت؛ أما الأشخاص المتحفظون فيستخدمون مفاتيح بطول 1024 بت؛ والمفاتيح بطول 2048 بت مناسبة للأشخاص الذين قد يصرحون عن المعلومات التي شفروها ولكن عندئذ سوف يقتلونك.

إن التشفير المتناظر مناسب جداً لتشفير البيانات، مثل الملفات، المجلدات والمستندات. والمشكلة مع التشفير المتناظر هي كونه أقل فائدة لإرسال الرسائل المشفرة. لا يمكنك أن تضمّن المفتاح مع الرسالة لأن أي شخص يستقبل الرسالة يمكنه أن يستخدم المفتاح لفك تشفيرها. (يفترض المشفرون دوماً أن أحد الأشخاص يتطفل عليهم). يمكنك أن تضع المفتاح

على قرص وترسله بالبريد، ولكنك تخاطر عندئذ بضياع القرص أو بسرقته. يمكنك أن تتفـــق على مكان تترك القرص فيه، لكن إذا كان المتطفّل يراقب اتصالاتك فسوف يعـــرف مكـــان القرص. وحتى لو كان بإمكانك أن تتفق على مكان تضع فيه القرص سراً، فما العمل إذا كان الشخص الذي تتصل معه يقطن في الطرف الآخر من البلاد؟ يمكنك أن تسلم الرسالة القرص شخصياً ولكن عندئذ يمكنك أن تسلم الرسالة أيضاً ولا تزعج نفسك بتشفيرها.

إن حل هذه المشكلة هو بالتشفير المتناظر، والذي يدعى أيضاً تشفير المفتاح العـــام. في تشفير المفتاح العام، يولد تابع رياضي واحد مفتاحين: يتم استخدام أحد هـــذين المفتـــاحين لتشفير النص البسيط، ويتم استخدام مفتاح منفصل لفك النص المشفر. ولا يمكن اســـتخدام مفتاح تشفير النص البسيط من أجل فك التشفير، والعكس بالعكس. وحقيقة كـــون هـــذه العملية ممكنة هو أمر مدهش بحد ذاته. يوجد خلفية رياضية معقدة للتشفير بالمفتاح العام (كما يتبين ذلك من أن الأشخاص الثلاثة الذين اكتشفوا خوارزمية المفتاح العام المشهورة، تـــدعى RSA، كانوا جميعاً في MIT). كل ما تحتاج أن تعرفه هو أنه يلزم مفتاحين لحل مشكلة تبادل المفتاح المتناظر بأمان.

إن مبدأ الفكرة كالتالي: تولد أليس زوج مفاتيح عامة. تحتفظ بأحد هذين المفتـــاحين لنفسها، وتنشر المفتاح الآخر في دليل عام على الإنترنت. إذا أراد بوب أن يرسل إلى ألـــيس رسالة مشفرة، يبحث عن مفتاحها العام في الدليل ويستخدمه لتشفير الرسالة. وعندما تستقبل أليس الرسالة، تستخدم مفتاحها الخاص لفك تشفيرها. إذا أرادت أليس أن تجيب بوب، تبحث عن مفتاح بوب العام وتستخدمه لتشفير الرسالة.

وكطبقة أمن إضافية، بدلاً من استخدام مفتاح أليس العام لتشفير الرسالة، يستخدم بوب مفتاح متناظر قوي لتشفير الرسالة ثم يستخدم مفتاح أليس العام لتشفير المفتاح المتنـــاظر. ثم يرسل كتلتي النص المشفر إلى أليس. وتستخدم أليس مفتاحها الخاص لفك تشـــفير المفتـــاح المتناظر ثم تستخدم المفتاح المتناظر لفك تشفير الرسالة.

التواقيع الرقمية والشهادات الرقمية

هل أصابتك الحيرة؟ إذا لم تصيبك بعد، فقد تصيبك الآن. يسمح تشفير المفتاح العـــام أيضاً باستخدام التواقيع الرقمية والشهادات الرقمية. يفيد التوقيع الرقمي في شـــيئين: الأول، يتحقق أن الرسالة قد وردت من الشخص الذي يدّعي بأنه قد أرسلها. والثاني، يمنع تزويـــر الرسالة.

لكي تنشئ أليس توقيعاً رقمياً، تأخذ رسالتها غير المشفرة وتطبق عليها خوارزمية مزج، وهي عملية رياضية تولد مزيج من الرسالة. ما هو جميل في خوارزمية المزج أنك إذا طبقتـــها على الرسالة ألف مرة، فسوف تحصل على مزيج الرسالة نفسه في كل مرة، ولكن إذا غيّرت

حرف واحد في الرسالة ثم طبقت خوارزمية المزج عليها، فسوف تحصل على مزيج رسالة مختلف. لذلك إذا أرسلت الرسالة ومزيج الرسالة (وخوارزمية المزج التي استخدمتها) إلى مستلمها، يمكنه عندئذ أن يطبق خوارزمية المزج نفسها على الرسالة. وإذا تطابق مزيجي الرسالة، يمكن أن يتأكّد مستلم الرسالة بأن الرسالة لم تتغير.

وبالتالي تطبق أليس خوارزمية المزج على رسالتها وتحصل على مزيج الرسالة. تأخذ مزيج الرسالة وتشفره مع مفتاحها الخاص. ثم يستخدم بوب مفتاح أليس العام لفك النص المشفر. يعلم بوب فك التشفير الناجح أن الرسالة قد أتت فعلاً من أليس، لأنها وحدها فقط تملك المفتاح الخاص. إن التواقيع الرقمية غير موجهة لحماية الرسالة من التجسس؛ فالتواقيع الرقمية تتحقق من صحة المرسل وتتحقق من سلامة الرسالة.

بالطبع توجد مشكلة مع تقنية المفتاح العام وهي أنه كيف يمكنك التحقق من أن صاحب المفتاح هو حقاً من يدّعي هويته. على سبيل المثال؛ لا يوجد شيء يمنع إيف من نشر مفتاحها العام وتسميته مفتاح أليس العام. وهكذا، يظن بوب بأنه يرسل رسالة محمية إلى أليس، لكنه يرسلها في الحقيقة إلى إيف. (وأنت كنت تظن أن فوكس مولدر عديم الثقة بالآخرين؟ إنه لم يحصل على أي علامة في مادة التشفير).

هنا يأتي دور الشهادات الرقمية. تحتوي الشهادة الرقمية على المفتاح العام لشخص أو مؤسسة. ويتم إصدار الشهادات الرقمية من جهة أخرى موثوقة (تدعى سلطة الشهادات)، وتعمل كأحد أشكال التحقق من الصحة لكي تتأكد بأن حامل الشهادة هو من يدّعي هويته. يمكنك أن تنظر إلى الشهادة الرقمية كشهادة القيادة. فيتم إصدارها من كيان موثوق وتقدم دليل قوي بشكل مقبول أنك أنت من تدّعي هويته.

بالطبع، حتى شهادات القيادة يمكن تزويرها، لذلك إذا كنت تتساءل لماذا تثق بالمؤسسة التي أصدرت الشهادة الرقمية، فإنك تتعلم الطريقة التي يفكر بها المشفر. لقد تم إصدار الشهادات الرقمية المزورة في الماضي، ومن المحتمل أن يحدث ذلك مرة أخرى. على كل حال، يجب أن لا تنتهي سلسلة الثقة (أو تبدأ) في مكان ما، والعديد من الشركات، بما في ذلك VeriSign، تقوم بعمل جيد كسلطة شهادات وتصدر الشهادات الرقمية في مجتمع الإنترنت.

ومع أن هذه الإجراءات تبدو معقدة وغير عملية في العالم الحقيقي، فإن تشفير المفتاح العام هو طريقة جيدة. وتعتمد بنية التجارة الإلكترونية الكاملة للإنترنت على تقنية المفتاح العام؛ في كل مرة تشتري شيئاً من Amazon.com أو تجري معاملة مصرفية على الوب، فإنك تستخدم بنية المفتاح العام.

يلعب تشفير المفتاح العام أيضاً دوراً مهماً في تشفير البريد الإلكتروني، والذي سوف نناقشه في الفقرة التالية.

تشفير البريد الإلكتروني

يدعى النموذج الأوسع انتشاراً لتقنية المفتاح العام من أجل تشفير البريـــد الإلكتـــروني PGP، ويعني خصوصية جيدة جداً وقد أنشأه فيل زيمرمان. كما أنه اسم الشركة التي تصنع برمجيات التشفير التجارية أيضاً، بما في ذلك PGP Desktop Home 9.0. يمكن استخدام هذا المنتج لتشفير رسائل البريد الإلكتروني الصادرة، الرسائل الفورية AOL، وبعض الملفات على كمبيوترك. ويدعم مايكروسوفت أوتلوك وThunderbird، مستضاف البريد الإلكتروني من مؤسسة Mozilla، التي تقدم برنامج استعراض الوب Firefox أيضاً. وهو متوفر على الوب في الموقع www.pgpstore.com.

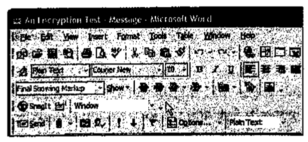
يمكنك أن تحمّل إصدار مجاني مفتوح المصدر من هذه البرمجيات يدعى Open PGP من www.pgpi.org. يجب أن تنقر عبر عدد من الصفحات لكي تجد إصدار ويندوز XP.

يمكنك أن تحصل أيضاً على برنامج تشفير البريد الإلكتـــروني مـــن شـــركة تـــدعى Hushmail. يستخدم هذا البرنامج المعيار Open PGP ويقدم إصدار بريد الوب وإصـــدار يعمل مع أوتلوك، مستضاف البريد الإلكتروني المبيت في مايكروسوفت أوفيس. يمكنك معرفة المزيد من www.hushmail.com.

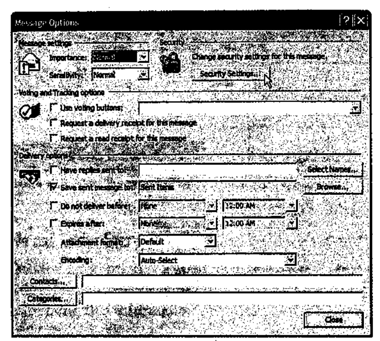
بالإضافة إلى البرمجيات الأخرى، فإن مستضاف البريد الإلكتروني أوتلوك الذي يأتي مع مايكروسوفت أوفيس يسمح بتشفير رسائل البريد الإلكتروني الصادرة. ويعتمد أيضاً على تقنية المفتاح العام، لذلك يجب أن تحمّل وتشتري شهادة رقمية. عندما تحاول إرسال رسالة مشفرة لأول مرة، تقودك مايكروسوفت عبر الخطوات الضرورية للحصول على هذه الشهادة الرقمية.

على كل حال، قبل أن تنفذ جميع الخطوات، اعرف أنه قد لا تكون قادراً علـــى إرســـال الرسائل المشفرة باستخدام أوتلوك ما لم ينشئ الأشخاص الذين تراسلهم تواقيع رقمية ويســـجلوها في دليل عام على الوب. وذلك لأنه، إذا كنت تتذكر من نقاشنا حول تشفير المفتاح العام، يحتـــاج المرسل لاستخدام المفتاح العام لمستلم الرسالة. إذا أمكنك إقناع الأشخاص الذين تراسلهم بشـــراء تواقيع رقمية خاصة بهم، فإليك الخطوات الضرورية لاستخدام تشفير البريد الإلكتروني في أوتلوك.

أولاً، افتح أوتلوك واكتب رسالتك. وبعد أن تصبح الرسالة جاهزة، انقر الـــزر Options، كما هو مبين في الشكل 10-1. وعندما يفتح الإطار Message Options، كما هو مبين في الشكل 10-2، انقر الزر Security Settings. فيفتح الإطار Security Properties، كما هو مـــبين في الشـــكل 10-3. دقـــق مربـــع التـــدقيق Encrypt message contents and attachments. يجب أن لا تدقق الآن مربـــع التـــدقيق Add digital signature to this message، لأنك تحتاج أن تثبت في البداية شهادة رقمية. انقر OK في مربع حوار خصائص الأمن. يجب أن يتم إعادتك إلى رسالتك. اختر عنواناً لكي ترسل الرسالة إليه.



الشكل (10-1): نقر الزر Options بعد كتابة الرسالة في أوتلوك.

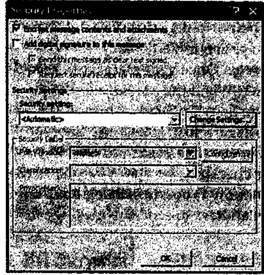


الشكل (10-2): مربع حوار خيارات الرسالة.

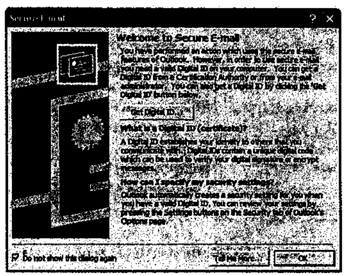
بعد أن كتبت رسالتك، انقر على الزر Send. ترى الإطار Welcome to Secure E-mail كما هو مبين في الشكل 10-4. انقر الزر ...Digital ID. فيأخذك إلى موقـع الـوب لمايكروسوفت مع ارتباطات إلى مزودات شهادات رقمية: VeriSign.

يسمح لك المحدد ID الرقمي الشخصي لـ GeoTrust بتوقيع مستندات وورد رقمياً وتوقيع وتشفير البريد الإلكتروني رقمياً. ويكلف 19.95$ في السنة.

يكلف المحدد ID الرقمي لـ VeriSign ‏19.95$ في السنة أيضاً. وتحصل على حماية تعادل 1000$ ضد الخسارة الاقتصادية في حال فساد، ضياع أو استخدام شهادتك الرقمية بشكل سيء. وتوردك VeriSign أيضاً في دليل عام بحيث يمكن لأي شخص يريد أن يرسل إليك رسالة مشفرة أن يجد مفتاحك العام. وتسمح أيضاً باستخراج الشهادات الرقمية الأخرى الصادرة عن VeriSign. وتقدم VeriSign أيضاً فترة تجريبية للشهادة الرقمية تبلغ 60 يوماً.



الشكل (10-3): مربع حوار خصائص الأمن.

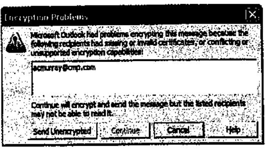


الشكل (10-4): مربع حوار الترحيب إلى البريد الإلكتروني الآمن.

يجب أن تسجل من أجل الحصول على الشهادة. تحتاج إلى بريـــدك الإلكتـــروني (وإلى خطك الهاتفي من أجل GeoTrust) من أجل عملية التسجيل. والتسجيل هو عملية بسيطة، تسألك عن اسمك وعنوان بريدك الإلكتروني. وبعد التسجيل، تنقر على زر التثبيت لتثبيـــت الشهادة الرقمية. وعندما تبدأ عملية التثبيت، قد تعرض مايكروسوفت تحذير بتعدي خطـــير للنصوص البرمجية. انقر Yes من أجل الاستمرار.

بعد أن تثبيت الشهادة الرقمية، يمكنك أن تنقر أخيراً الـــزر Send في مايكروســـوفت أوتلوك. على كل حال، كما ذكرنا، قد تعترضك عقبات إذا كان الأشخاص الذين ترســـل

إليهم الرسائل المشفرة لا يملكون شهادات رقمية (انظر إلى الشكل 10-5). بالإضافة إلى ذلك، لا تدعم بعض أنظمة البريد أوأنها ألغت تأهيل S/MIME (ملحقات بريد الإنترنت الآمنة/متعدد الأغراض، معيار تشفير بمفتاح عام) أو قد لا تقبل الرسائل المشفرة لأن المواسح المضادة للفيروسات لا يمكنها أن تمسح البريد الإلكتروني المشفر.



الشكل (10-5): مربع حوار مشاكل التشفير.

تشفير الملفات والمجلدات

إن تشفير سطح المكتب هو فكرة جيدة إذا كنت تحفظ معلومات حساسة، مثل العائدات الضريبية على الوب، أرقام الحسابات، وهكذا على كمبيوترك. وخصوصاً، يقدم تشفير هذه المعلومات بعض الحماية في حال سرقة أو ضياع كمبيوترك. (حسب استطلاع في 2001، تم نسيان آلاف من الكمبيوترات المحمولة في عربات وسائل النقل في لندن).

تعمل معظم منتجات التشفير المكتبية بالشكل نفسه. تشير إلى ملف أو مجلد لتشفيره. لكي تفك التشفير، يتم توجيهك لتقديم كلمة مرور. وبهذه الطريقة يعمل Icon Lock-iT XP. اذهب إلى www.icon lockit.com للحصول على المزيد من المعلومات. كما ذكرنا، يتضمن PGP Desktop تشفير البريد الإلكتروني والملفات. يمكنك أن تجد أدوات التشفير على الوب. على سبيل المثال، تقدم PC Magazine أداة تشفير تدعى File Warden. لكي تحصل على تحميل مجاني، اذهب إلى pcmagazine.com وابحث عن File Warden 2.

مقنّعات الوب

يمكن أن تساعد مقنّعات الوب في حماية خصوصيتك عندما تستخدم الإنترنت. تزيل منتجات تقنيع الوب المعلومات التي يمكن استخدامها لتحديد هويتك ولتعقب عاداتك في التجول على الوب. كما أنها توجه حركة المرور على الوب عبر مختلف الموجهات والملقمات لإخفاء المصدر والوجهة (يدعى أحياناً توجيه البصلة). يقدم مركز الديمقراطية والتكنولوجية لائحة طويلة بخدمات تقنيع الوب في www.cdt.org/resourcelibrary/Privacy/Tools/Anonymizer.

يمكنك أن تدقق أيضاً برنامج تقنيع يدعى Tor، تموله مؤسســة الحـدود الإلكترونيـة (EFF)، مجموعة محاماة حقـوق الخصوصـية. لكـي تـتعلم المزيـد عنـه اذهـب إلى http://tor.eff.org/.

هناك خيار آخر هو Privoxy، في www.privoxy.org. إن Privoxy هو ملقم وكيل للوب يمكنه أن ينـزع الإعلانات، الملصقات الدعائية والأطر المنبثقة ويدير الكعكات. والملقم الوكيل هو كمبيوتر يتوسط وصلات الإنترنت للكمبيوترات. أي أنه بدلاً من الذهاب مباشرة إلى ملقم الوب لتحميل صفحة وب، يمكنك أن تذهب إلى الملقم الوكيل. والملقـم الوكيـل يذهب إلى الملقم ويحمّل صفحة الوب من أجلك. كما إنه يعيق كعكات التعقب أيضاً. وبالتالي لا يمكن لملقم الوب أن يضع كعكة على كمبيوترك لأن كمبيوترك لم يزر صفحة الوب أبداً.

وتوجد طريقة أخرى للحصول على بعض الخصوصية على الإنترنـت وهـي بإزالـة كعكات التعقب من كمبيوترك. فكعكات التعقب تسجل مواقع الوب التي تزورها والإعلانات التي تنقر عليها في ملف نصي تحفظه على كمبيوترك. يتم استخدام كعكات التعقب لتجميـع المعلومات عن عاداتك في التجول على الوب من أجل تسليم الإعلانات الموجهـة وتجميـع إحصائيات عن صفحات الوب التي تزورها. تضع جميع مواقع الوب التي تزورها كعكات على كمبيوترك لمساعدة ملقم الوب على تذكر متى زرت الموقع ومن أجل تخصيص بيئة موقع الوب بتذكر أفضلياتك وإعداداتك. على كل حال، تشارك كعكات التعقب هذه المعلومـات مـع جهات أخرى. لن تؤذي هذه الكعكات كمبيوترك، لكنها تمثّل تـدخلاً في خصوصـيتك. يمكنك أن تكشف، تزيل، وتحجز كعكات التعقب باستخدام البرمجيات المضـادة للسـبايوير (انظر إلى الفصل الخامس، "التخلص من الضيوف غير المرغوبين، الجزء 2: سبايوير، أدويـر وأحصنة طروادة").

2-10 التعامل مع سماسرة البيانات

تجمع سماسرة البيانات مثل ChoicePoint، LexisNexis وAcxiom حجوم لا تصدق من المعلومات تتعلق بنا. وتنجز هذه الشركات تجميع بياناتها من المصادر العامة، مثل دلائـل الهاتف وسجلات المبيعات المنـزلية العامة، والتي هي عبارة عن معلومات عامة. لكنها تحصل على المعلومات أيضاً من مصادر أخرى. على سبيل المثال، تحصل Acxiom على كثير مـن المعلومات من الشركات التي تريد أن تنقب في تلك المعلومات لكي تتعلم المزيد عن زبائنـها. وحسب الكاتب Robert Harrow، jr. في كتابه لا يوجد مكان للاختباء فإن الشركات بما في ذلك Sears، Hallmark Cards، Safeway وLands End ترسل جميعها المعلومات التي جمعتها عن زبائنها إلى Acxiom. وفوق ذلك ترسل شركات المصارف وبطاقات الائتمـان بياناتها إلى قواعد بيانات Acxiom.

إن المشكلة أمام المستهلكين هي أنه طالما تتخذ خطوات لتحديد المعلومات التي تقدمها إلى الأعمال الفردية والوكالات الحكومية، فإن هذه المؤسسات نفسها يمكنها أن تحمّل جميع أجزاء المعلومات المتفرقة عنك في نظام كمبيوتر كبير يمكنه أن يربط ويحلل كميات هائلة من المعلومات.

لكي تتجنب حفظ ملف عنك، يجب أن تحفظ المعلومات عن نفسك بعيداً عن السجل العام قدر الإمكان. يقدم كريس هوفنيل، مدير الشاطئ الغربي لمركز معلومات الخصوصية الإلكترونية (EPIC)، منظمة محاماة الخصوصية، التوصيات التالية:

- إذا بعت أو اشتريت منزلاً، تأكد أن رقم الضمان الاجتماعي وتاريخ الولادة لا يظهران في السجل العام.
- عندما توقع من أجل الخدمة الهاتفية والأدوات العامة، اطلب بإصرار أن لا تستخدم الشركة رقم ضمانك الاجتماعي أو رقم شهادة القيادة. وقد تضطر إلى إيداع مبلغاً إذا قررت أن تسلك هذا الطريق.
- لا تعرض نفسك للتوقيف لأنه يتم تعميم سجلات التوقيف.

يمكنك أن تتخذ خطوات أيضاً لتحديد ما الذي تفعله سماسرة البيانات مع المعلومات، وفي بعض الحالات يمكنك الوصول إلى المعلومات التي تحفظها عنك، إزالة معلوماتك من قواعد البيانات أو طلب إزالة المعلومات.

(www.acxiom.com) Acxiom

تقدم Acxiom مجموعتين أساسيتين من المنتجات: InfoBase marceting، وInfoBase and Sentricx Reference. تستخدم مستضافات Acxiom المنتج InfoBase Marketing لكي تنشئ لوائح من أجل الإعلانات الموجهة. لا يتضمن المنتج InfoBase Marketing أي معلومات طبية أو ائتمانية أو أرقام الضمان الاجتماعي. ويمكنك أن تزيل معلوماتك من قاعدة البيانات InfoBase Marketing، ويعني ذلك أن الأعمال التي ترعاها لا يمكنها أن تصل إلى المعلومات عبر Acxiom، ولن تتلقى اتصالات تسويقية، بريد مباشر (بريد تافه)، كتالوجات أو بريد إلكتروني من الشركات التي تتعامل مع Acxiom. يمكنك أن تطلب نموذج إلغاء الاشتراك بالاتصال بالرقم 501-342-2722 أو 877-774-2094 أو بإرسال بريد إلكتروني إلى optoutUS@acxiom.com.

تتضمن الخدمات InfoBase من Acxiom وSentricx Reference معلومات مالية وأرقام الضمان الاجتماعي. وتستخدم مستضافات Acxiom هذه الخدمات من أجل مراقبة الموظفين وتحرير العقود. ويمكن أن تصل أقسام الشرطة أيضاً إلى المعلومات InfoBase و Sentricx Reference. يمكنك أن تصل إلى المعلومات المحفوظة عنك بطلب تقرير معلومات مرجعي. لاحظ

أن Acxiom تطلب أجرة 5$. يمكنك طلب التقرير بالاتصال بـالرقم 501-342-2722 أو 877-774-2094 أو بإرسال بريد إلكتروني إلى referencereport@acxiom.com.

لكي تحصل على مزيد من المعلومات، اذهب إلى www.acxiom.com وانقر الارتباط Privacy على الجانب الأيسر من صفحة البدء. يمكنك أن تكتب أيضـاً Access، Notice، Choice (كما كتبت هنا) في حقل البحث في صفحة البدء لكي نعرف المزيد عن الوصول إلى المعلومات التي تجمعها Acxiom عنك.

ChoicePoint (www.choicepoint.com)

يخصص مرسوم المعاملات الإئتمانية العادلة والدقيقة (FACT) المستهلكين بتقرير مجاني سنوي من وكالات تقرير المستهلكين، ووفقاً للمؤسسة ChoicePoint فإن ثلاثاً من خدماتها يقع ضمن المرسوم FACT: C.LU.E، الذي يتعقب المعلومـات عـن عمليـات التـأمين وسجلاتها؛ ChoicePoint WorkPlace Solutions، الـتي تغطـي التـاريخ الـوظيفي؛ وResident Data، التي تحفظ معلومات القاطنين. وتحت رقابة المرسوم FACT، يجـب أن تقدم ChoicePoint عند الطلب نسخة مجانية واحدة في السنة عن ملف المستخدمين من جميع وحدات العمل المذكورة. لاحظ أن وحدات العمل المذكورة قد لا تملك ملف مستخدم عنك. على كل حال، إذا أردت التدقيق، فلديك الخيارات التالية (يمكنك أن تحصل على المزيد مـن المعلومات في www.choicepoint.com/factact.html):

- لكي تطلب نسخة عن تقرير سجل المطالبة، اذهـب إلى www.choicepoint.com أو اتصل بالرقم 866-312-8076. claim
- لكي تطلب نسخة عن تقرير السجل الوظيفي، اتصل بالرقم 866-312-8075.
- لكي تطلب نسخة عن تقرير سجل الإقامة، اتصل بالرقم 866-448-5732.

يمكنك أن تطلب هذه المعلومات أيضاً بالبريد النظامي. يجب أن ترسل اسمك وعنوان ووحدات العمل المناسبة المذكورة هنا. فيرسلون نموذج الطلب الذي يجـب أن تكتبـه وتعيده.

من أجل تقارير سجل المطالبة:

ChoicePoint Consumer Disclosure Center

P.O.Box 105295

Atlanta,GA 30348

من أجل تقارير السجل الوظيفي:

ChoicePoint WorkPlace Solutions Consumer Disclosure Center

P.O.Box 105292

Atlanta,GA 30348

من أجل تقارير سجل الإقامة:

Resident Data Consumer Disclosure Center

P.O.Box 850126

Richardson,TX 75085-0126

(www.lexisnexis.com) LexisNexis

يقدم LexisNexis معلومات عن الأعمال والقوانين والمخازن، السجلات العامة وأكثر من ذلك. ويمكن أن تعرف المعلومات غير العامة المخزنة عنك بطلب نسخة عنها. يكلف LexisNexis $8 لقاء هذه الخدمة. لكي تطلب نسخة عن هذه المعلومات، اكتب إلى:

LexisNexis Consumer Access Program

P.O.Box 933

Dayton, OH 45401

يجب أن تضع $8 مع طلبك. ويجب أن تذكر اسمك، وكنيتك وأي أسماء أخرى تستخدمها. يمكنك أن تكتب رقم الضمان الاجتماعي، حيث تقول LexisNexis بأنه يساعد على كتابة طلب المعلومات. على كل حال، رقم الضمان الاجتماعي خياري. من أجل مزيد من المعلومات عن الحصول على المعلومات الشخصية. اذهب إلى www.lexisnexis.com/terms/privacy/data/obtain.asp.

يمكنك أن تطلب من LexisNexis أن تزيل اختيارياً السجلات غير العامة المتعلقة بك. على كل حال، تصر الشركة على تحقيق أحد ثلاثة شروط: يجب أن تكون ضابط شرطة تسببت بحفظ معلوماتك في قاعدة البيانات، يجب أن تكون ضحية سرقة الهوية ولديك نسخة عن الشهادة الخطية بالسرقة (انظر إلى الفصل الثاني لمزيد من المعلومات) أو يجب أن تكون عرضة لأذى فيزيائي ولديك أمر محكمة أو تقرير شرطة لتثبت ذلك. لكي تجد المزيد عن تحقيق هذه الشروط وطلب إزالة المعلومات، اذهب إلى www.lexisnexis.com/terms/privacy/data/remove.asp.

10-3 لائحة التدقيق

استخدم هذه اللائحة كدليل مرجعي للمواد المغطاة في هذا الفصل.

ما يجب أن تفعله

- تشفير البريد الإلكتروني لحماية رسائلك من التجسس.

- استخدام متعقبات الوب أو الملقمات الوكيلة لإخفاء نشاطات التجول على الوب.
- محاولة إبقاء رقم الضمان الاجتماعي وتاريخ الولادة بعيداً عن السجلات العامة.
- تدقيق الملفات التي قد يتم حفظها عنك لدى سماسرة البيانات الرئيسية.
- إلغاء الاشتراك ببرامج مشاركة المعلومات لدى سماسرة البيانات كلما أمكن ذلك.

ما يجب أن لا تفعله

- تزويد السجلات العامة بمعلومات حساسة كلما أمكن الأمر.
- نسيان أنك ومراسليك تحتاجون إلى التوقيع من أجل الشهادات الرقمية لاستخدام أنظمة تشفير المفتاح العام.

4-10 موارد مساعدة

يقدم هذا القسم موارد إضافية لمساعدتك على تعلم المزيد.

إن مركز معلومات الخصوصية الإلكترونية (EPIC) هو مجموعة بحث عامة تدرس الحريات المدنية وأمور الخصوصية. ينشر المركز تقارير وكتب عن الخصوصية والحكومات والخطابات. يتم اختبار أعضاء WPIC غالباً أمام اللجان الفيدرالية حول تشريعات الحريات المدنية والخصوصية. ويقدم موقع الوب EPIC عدداً كبيراً من القصص والمعلومات حول أمور الخصوصية. وهناك صفحتان مهمتان على وجه الخصوص تقدمان أدوات خصوصية الإنترنت. اذهب إلى الموقع www.epic.org/privacy/tools.html. لاحظ أن EPIC لا تصادق على أي من الأدوات المذكورة. إنها ببساطة عينة من الأدوات المتوفرة. يجب أن تدقق أيضاً أحكام خصوصية المستهلكين العشرة الأولى. اذهب إلى www.epic.org/privacy/2004tips.html.

إن مركز الديمقراطية والتقنية هو مجموعة محاماة غير ربحية تعمل لحماية حريات المدنيين، وعلى الأخص التعبير بحرية والخصوصية. يتم اختبار أعضاء CDI بشكل دوري أمام الكونغرس عن الأمور المهمة مثل الخصوصية، التعبير بحرية، وحقوق النسخ. وموقع الوب هو مورد رائع للاطلاع على التشريعات. سوف تجد كتب ومقالات وأخبار بالإضافة إلى ارتباطات للاتصال مع أعضاء مجلس الشيوخ والمجلس التمثيلي بخصوص مختلف الأمور. اذهب إلى www.cdt.org.

مؤسسة الحدود الإلكترونية (EFF) هي مؤسسة غير ربحية أخرى تعمل لحماية حرياتنا في هذا العالم التقني. تتابع EFF قضايا أخرى مثل الخصوصية، حقوق النسخ، مشاركة الملفات، التصويت الإلكتروني وهكذا. يمكنك أن تجد المزيد في الموقع www.eff.org.

دار بيانات حقوق الخصوصية هو مورد للمعلومات عن خصوصية الإنترنت، الخصوصية

المالية، ومواضيع أخرى. تقدم توصيات لحماية خصوصيتك وتتعقب التشريعات الفيدرالية المتعلقة بالخصوصية. اذهب إلى www.privacyrights.org.

كتاب الترميز: علم الأسرار من مصر القديمة إلى التشفير الكوانتي، للكاتب سيمون سينغ، هو مقدمة ممتازة عن التشفير حقق كثيراً من المبيعات. يتتبع سينغ أصول التشفير وتحليل التشفير حتى يومنا الحاضر. ويستعرض الدور التاريخي الذي لعبه التشفير في موت ملكة سكوتلاند ماري، نصر القوى المتحالفة في الحرب العالمية الثانية، تطور علم الكمبيوترات الحديث، إنشاء التشفير بالمفتاح العام وPGP، والمعركة الحالية بين الحكومات التي تعرف بتوفر تقنيات التشفير للعموم والباحثين الذين يحذورون من مراقبة الحكومة.

لا مكان للاختفاء: خلف كواليس مجتمع المراقبة الناشئ، للكاتب روبرت أوهارو، .jr، يضيء عملية تجميع البيانات التجارية والحكومية ويستكشف كيف تتعاون القطاعات الحكومية والخاصة لإنشاء بنية تحتية وطنية استخباراتية.

ثرثرة: رسل من العالم السري للتجسس العالمي، للكاتب باتريك راون كيفي، يستكشف أعماق المراقبة الحكومية الشاملة ولغز الأمن والخصوصية. وهو مقدمة من الطراز الأول عن Echelon، نظام المراقبة الإلكترونية الشاملة الذي تشغله NSA وتم تطويره من الولايات المتحدة، بريطانيا، كندا، أستراليا ونيوزلاندا.

الخاتمة

شكراً لقراءة هذا الكتاب. نأمل أن يكون قد ساعدك بفهم المخـاطر الأمنيـة علـى الإنترنت وقدم بعض المعلومات العملية حول حمايتك وعائلتك على الوب.

إن التجول على الوب يمكن أن يكون آمناً كالتجول قرب المنـزل. فيمكنك أن تتجنب العديد من المآزق والأخطار التي تؤدي إلى خسائر مالية، ضـياع البيانـات، وتخفـيض أداء الكمبيوتر أو إلى مجرد التعرض لإزعاج شخصي، وذلك باستخدام الأدوات الصحيحة وتلقي التدريب المناسب.

تحتل السبايوير، السبام والخدع على الإنترنت في هذه الأيام عناوين الصحف. لكـن التقنية تتغير باستمرار، والمستقبل سيكشف عن مخاطر وتهديدات جديدة مع ظهور البرمجيـات الأحدث والإمكانيات الجديدة. ولكن الأخبار الجيدة هي أن الممارسات والنصـائح الجيـدة المذكورة في هذا الكتاب تنطبق على التهديدات الجديدة بالإضافة إلى المخاطر التي تحدثنا عنها في الفصول السابقة.

وكتذكير أخير، نذكر الخطوات الخمسة الأساسية التي يمكنك اتخاذها وتجعل كمبيوترك آمناً في مواجهة هجمات اليوم والغد:

1. استخدم إجرائية أمنية على الإنترنت تجمع بين البرمجيات المضادة للفيروسات، البرمجيـات المضادة للسبايوير، جدار نار، كشف التدخل، وإدارة نقاط الخلل من أجل الحصول على الحماية القصوى ضد التهديدات المتنوعة. وحافظ على تحديث خدمة الاشتراك الأمنيـة فتستقبل تعاريف الفيروسات والسبايوير الحديثة.
2. حدّث نظام التشغيل وبرنامج الاستعراض بشكل دوري. وتذكر أن كل ثاني ثلاثاء من كـل شهر هو ثلاثاء الرقع، حيث تصدر مايكروسوفت الرقع البرمجية الأحـدث. احـرص علـى الحصول على هذه التحديثات وتثبيتها بشكل فوري أو أهّل الوظيفة Automatic Updates في Windows XP. تذكر أيضاً أن تستخدم كلمات المرور المؤلفة من حروف وأرقام.

3. لا تأكل الحلويات من الغرباء. نقصد بذلك أنه يجب أن تكون متشككاً أو على الأقــل حذراً، عند استخدام الإنترنت. احذر خصوصاً من البرامج المجانية التي تعد بتقديم أمــور مسلية أو مساعدة. واشتبه كثيراً بالبريد الإلكتروني. لا تفتح الرسائل من الأشخاص الذين لا تعرفهم. وإذا فتحت رسائل من أشخاص لا تعرفهم، لا تؤهل أو تحمّل أو تنقــر أي ملحق بهذا البريد الإلكتروني. لا ترسل المعلومات الحساسة بالبريد الإلكتروني مثل كلمات المرور، أرقام بطاقات الاعتماد والحسابات المصرفية أو رقم الضمان الاجتمــاعي إلى أي شخص، أبداً.
4. لا تشتر أي شيء من مرسل السبام. يجب أن تعلم بالأخطار المرتبطة مع شراء البرمجيات – أو أي منتج – عن طريق البريد الإلكتروني المشبوه. يمكن أن تأتي البرمجيات مع فيروسات أو علل قد تكون مخربة لنظام التشغيل في الكمبيوتر. لا توقّع من أجل تسجيل الدخول إلى مواقع وب غير معروفة تعدك بإزالة اسمك من لوائح السبام، ولا تنقر علــى الارتبــاط "remove from mailing list" في البريد الإلكتروني؛ فمرسلو السبام يستخدمون هــذه الخدع للتحقق والحصول على عناوين البريد الإلكتروني.
5. انسخ الملفات الأساسية احتياطياً بشكل دوري لكي تبقى بياناتك موجودة عند حدوث مشكلة كبيرة في الكمبيوتر. يمكنك حفظ الملفات على الأقراص المضــغوطة، ســواقات الفلاش أو في خدمة حفظ على الوب.

إن القواعد الخمسة تتضمن أمور كثيرة، ويمكننا تقليصها إلى قاعدة واحدة: استخدام حدسك العام. فالإنترنت ليست صديقتك. إنها مجتمع، وكأي مجتمع، يشكل المجرمــون والمحتالون نسبة من تعداده. ويجب أن لا تتجنب الإنترنت أبداً؛ بدلاً من ذلك تصــرف كأنك غريب في البلدة – ابقِ عينيك مفتوحتان، استخدم رأسك، وابقِ إحدى يديك على محفظتك.



Addison-Wesley

دليل سيمانتك إلى أمن الإنترنت في المنزل

احمِ نفسك! مساعدة سهلة بطريقة الخطوة خطوة من صانع أكثر أنظمة الأمان ثقة في العالم

تتغلغل الإنترنت بيننا ومعها تنتشر أخطارها، فإذا كنت تتبضّع أو تنفّذ معاملاتك المصرفية على الشبكة، أو حتى لو كنت تتصفح عبر المواقع وتستخدم البريد الإلكتروني، فإنك معرّض للقراصنة، واللصوص، وأخصائيي الاحتيال، ففي هذه الأيام لا حاجة للصوص أن يخلعوا الأقفال أو يكسروا الزجاج في منزلك ليسرقوه، فما عليهم سوى مهاجمتك أنت وعائلتك عبر شبكة الإنترنت. فهل أنت مستعد؟

احصل على الأمان الشبكي عبر مساعدة سهلة بطريقة الخطوة خطوة من شركة سيمانتك صانع أكثر أنظمة الأمان ثقة في العالم.

يساعدك هذا الكتاب السهل الفهم لحماية نفسك ضد تهديدات الإنترنت. ولأنه مؤلّفٌ خصيصاً للمستخدمين العاديين، فإنك ستتعلم طرقاً بسيطة للمحافظة على أمانك وأمان عائلتك على الشبكة.

- حافظ على حاسوبك بمنأى عن برامج التجسس، والتلصص، وديدان الخرق، والفيروسات والمقتحمين.
- احمِ هويتك وخصوصيتك.
- أبحر في عباب الإنترنت بأمان وتخلص من البريد المتطفّل في صندوق بريدك.
- إدفع بالمتطفلين بعيداً عن شبكتك اللاسلكية.
- استفد من مميزات الأمان الجديدة المبيّنة في نظام ويندوز إكس بي.
- احمِ أولادك من محتويات الإنترنت البذيئة والمستغلين على الشبكة.
- احمِ خدمة هاتفك العاملة على الإنترنت.
- إحصل على أدوات مجانية تساعدك في المحافظة على أمان حاسوبك.

أندرو كونري موراي المحرر التقني لمجلة IT Architect مختص بالكتابة حول أمن الإنترنت. ولقد ظهرت مقالاته كذلك في مجلتي Internet Week وNetwork Computing.

فنسنت ويفر المدير الأول المسؤول عن تقصّي الأمان في شركة سيمانتك، وهو يقود فريقاً من اخصائيي الأمان في أبحاثهم حول التهديدات الحديثة للإنترنت ولتقديم أفضل التصديات وأوثقها وأسرعها لمواجهة جميع انتهاكات أمان الشبكة العنكبو... حلولاً وخدمات ...كات للمحافظة على ...يتها بشكل متكامل





الدار العربية للعلوم
Arab Scientific Publishers
www.asp.com.lb

ص. ب. 13-5574 شوران 2050-1102 بيروت – لبنان
هاتف: 785107/8 (1-961+) فاكس: 786230 (1-961+)
البريد الإلكتروني: asp@asp.com.lb